HANDBOOK OF TERRORISM PREVENTION AND PREPAREDNESS

EDITED BY ALEX P. SCHMID
Handbook of Terrorism Prevention and Preparedness

Edited by Alex P. Schmid
About ICCT

The International Centre for Counter-Terrorism – The Hague (ICCT) is an independent think and do tank providing multidisciplinary policy advice and practical, solution-oriented implementation support on prevention and the rule of law, two vital pillars of effective counter-terrorism.

ICCT’s work focuses on themes at the intersection of countering violent extremism and criminal justice sector responses, as well as human rights-related aspects of counter-terrorism. The major project areas concern countering violent extremism, rule of law, foreign fighters, country and regional analysis, rehabilitation, civil society engagement and victims’ voices.

Functioning as a nucleus within the international counter-terrorism network, ICCT connects experts, policymakers, civil society actors and practitioners from different fields by providing a platform for productive collaboration, practical analysis, and exchange of experiences and expertise, with the ultimate aim of identifying innovative and comprehensive approaches to preventing and countering terrorism.

Licensing and Distribution

ICCT publications are published in open access format and distributed under the terms of the Creative Commons Attribution-Non Commercial No Derivatives License, which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

Copyright holders

Alex P. Schmid for selection and editorial matters and chapters 1, 2, 18, 24, 27 and 35; individual contributors for other chapters. The right of the editor to be identified as the author of the editorial material, and of the authors for their individual chapters, has been asserted in accordance with sections 77 and 78 of the Copyright, Design and Patents Act 1988.

All rights reserved. This is an Open Access Publication. Parts or the whole of the Handbook of Terrorism Prevention and Preparedness may be freely reproduced and redistributed, electronically, mechanically or by other means as long as this is not done for profit or on a commercial basis. ICCT wishes to be informed about reproduction and redistribution in English or other languages of individual chapters of the entire Handbook of Terrorism Prevention and Preparedness.
“There needs to be a renewed and sustained focus on prevention, including addressing the underlying conditions that cause young men and women to be lured by terrorism. This includes preventing conflicts, addressing fragility, strengthening state institutions and civil society, building durable peace and promoting sustainable development to tackle the poverty, inequality and lack of opportunity that feed despair.”

- UN Secretary-General António Guterres’ remarks to the African Regional High-Level Conference on Counter Terrorism and Prevention of Violent Extremism Conducive to Terrorism, 10 July 2019.
Handbook of Terrorism Prevention and Preparedness

List of Contributors xiii

Foreword xxv
Alexander von Rosenbach

Acknowledgements xxix

Frameworks for Analysis

Chapter 1: Introduction: Purpose and Organization of the Handbook
Alex P. Schmid 1

Chapter 2: Terrorism Prevention: Conceptual Issues (Definitions, Typologies and Theories)
Alex P. Schmid 13

Part I: Lessons for Terrorism Prevention from Related Fields

Chapter 3: A Criminological Approach to Preventing Terrorism: Situational Crime Prevention and the Crime Prevention Literature
Kelly A. Berkell 49

Chapter 4: De-Exceptionalizing the Terrorist Phenomenon: Lessons and Concepts from Conflict Prevention and Transformation
Andreas Schädel and Hans J. Giessmann 75

Chapter 5: Contributions from the Military Counter-Insurgency Literature for the Prevention of Terrorism
Rob de Wijk 109

Chapter 6: ‘Killing Them to Save Us’: Lessons from Politicide for Preventing and Countering Terrorism
Clark McCauley 139

Part II: Prevention of Radicalization

Chapter 7: At the Crossroads: Rethinking the Role of Education in Preventing and Countering Violent Extremism
Thomas K. Samuel 165

Chapter 8: Prevention of Radicalization to Terrorism in Prisons: A Practical Guide
Gary Hill 207
Chapter 9: Prevention of Radicalization to Terrorism in Refugee Camps and Asylum Centers  
*Barbara H. Sude*  
238

Chapter 10: Preventing Terrorism from Students of Extremist Madrasahs: An Overview of Pakistan’s Efforts  
*Asad Ullah Khan and Ifrah Waqar*  
270

Chapter 11: Prevention of Radicalization in Western Muslim Diasporas  
*Nina Käsehage*  
290

Chapter 12: Prevention of Radicalization on Social Media and the Internet  
*Sara Zeiger and Joseph Gyte*  
358

Chapter 13: Prevention of Recruitment to Terrorism  
*Ahmet S. Yayla*  
396

**Part III: Prevention of Preparatory Acts**

Chapter 14: Prevention of Terrorist Financing  
*Jessica Davis*  
444

Chapter 15: Prevention of Cross-Border Movements of Terrorists: Operational, Political, Institutional and Strategic Challenges for National and Regional Border Controls  
*Sajjan M. Gohel*  
474

Chapter 16: Prevention of the Procurement of Arms and Explosives by Terrorists  
*Mahmut Cengiz*  
508

Chapter 17: Prevention of CBRN Materials and Substances Getting into Terrorist Hands  
*Ioannis Galatas*  
532

Chapter 18: Prevention of (Ab-)Use of Mass Media by Terrorists  
*Alex P. Schmid*  
564

Chapter 19: Prevention of (Ab-)Use of the Internet for Terrorist Plotting and Related Purposes  
*Branislav Todorovic and Darko Trifunovic*  
594

Chapter 20: The Role of Intelligence in the Prevention of Terrorism (Early Warning – Early Response)  
*Ken Duncan*  
620
Part IV: Prevention of, and Preparedness for, Terrorist Attacks

Joshua Sinai 652

Annelies Pauwels 678

Chapter 23: Prevention of Bomb Attacks by Terrorists in Urban Settings: Improvised Explosive Devices
Rachel Monaghan and David Mcllhatton 704

Chapter 24: Prevention of Kidnappings and Hostage-Takings by Terrorists
Alex P. Schmid 732

Chapter 25: Preventing Suicide Attacks by Terrorists
Susanne Martin 764

Chapter 26: The Terrorist Threat to Transportation Targets and Preventive Measures
Brian Michael Jenkins 790

Chapter 27: Layers of Preventive Measures for Soft Target Protection Against Terrorist Attacks
Alex P. Schmid 816

Chapter 28: Prevention of Terrorist Attacks on Critical Infrastructure
Anneli Botha 841

Chapter 29: Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness. With Three Case Studies on Estonia, Singapore and the United States
Shashi Jayakumar 871

Chapter 30: Prevention of Lasting Traumatization in Direct and Indirect Victims of Terrorism
Shannon Nash 931

Part V: Preparedness and Consequence Management

Chapter 31: Prevention of Public Panic in the Wake of Terrorist Incidents
Juan Merizalde, John D. Colautti, and James J.F. Forest 963

Richard J. Chasdi 985

Chapter 33: Prevention of Revenge Acts and Vigilantism in Response to Acts and Campaigns of Terrorism
Marie Robin 1027
Chapter 34: Prevention of Human Rights Violations and Violations of International Humanitarian Law while Fighting Terrorism  
Tom Parker

Conclusions

Chapter 35: Conclusions: Terrorism Prevention – The UN Plan of Action (2015) and Beyond  
Alex P. Schmid

General Bibliography on Terrorism Prevention and Preparedness  
Ishaansh Singh

Index
List of Contributors

Alex P. Schmid is Editor of the Handbook of Terrorism Prevention and Preparedness and author of chapters 1, 2, 18, 24, 27 and 35. Dr. Schmid is a Research Fellow at the International Centre for Counter-Terrorism (ICCT) in the Hague, the Netherlands. He is Editor-in-Chief of Perspectives on Terrorism and former Co-Editor of Terrorism and Political Violence – both leading journals in the field of Terrorism Studies. Until 2009, Prof. em. Schmid held a chair in International Relations at the University of St. Andrews where he was also Director of the Centre for the Study of Terrorism and Political Violence (CSTPV). Previous positions include Officer-in-Charge of the Terrorism Prevention Branch of the UN Office on Drugs and Crime in Vienna and a chair in Conflict Resolution at the Erasmus University Rotterdam. Between 1978 and 2018 he also held various positions at Leiden University. Currently, he is Director of the Vienna-based Terrorism Research Initiative (TRI), a consortium of 16 institutes and more than 100 individual scholars seeking to enhance human security through collaborative research. Alex Schmid has more than 200 publication and reports in ten languages to his name, including the award-winning volume Political Terrorism (1984, 1988, 2006) and the Routledge Handbook of Terrorism Research (2011, 2013).

Kelly A. Berkell is author of chapter 3. Dr. Berkell is an Attorney and a Senior Research Fellow at the Center on Terrorism at John Jay College of Criminal Justice, City University of New York. She previously served as the National Security Fellow at Fordham Law School’s Center on National Security, focusing on terrorism and cybersecurity. A graduate of New York University School of Law and Barnard College, As Attorney, Kelly Berkell previously practiced securities and white-collar criminal litigation, and served as Legislative Counsel to a New York State Assembly Member. Her current research focuses on preventing and countering violent extremism, particularly where initiatives intersect with US laws and the criminal justice system. Her writing on these topics has appeared in the Harvard National Security Journal and the Journal for Deradicalization.

Anneli Botha is author of chapter 28. Dr. Botha is a Senior Lecturer at the Department Political Studies and Governance at the University of the Free State in Bloemfontein, South Africa. She also serves as an independent consultant on radicalization, deradicalization, reintegration and terrorism in Africa. In the period 2003 – 2016, she worked as a senior researcher on terrorism at the Institute for Security Studies (ISS) in Pretoria, South Africa. She has travelled extensively throughout Africa where she conducted research on terrorism and delivered specialized training on various aspects of the threat of terrorism, extremism, radicalization and counter-terrorism to law enforcement and criminal justice officials on the continent. Prior to her position at the ISS, she served in the South African Police Service (SAPS) for 10 years. Highlights included being a founding member of the Religious Extremism and Terrorism Desk at the Crime Intelligence Head Office and serving in the Rapid Reaction Unit and the Special Task Force on Urban Terror in the West Cape. At the end of her police career she provided strategic support to the Head of South Africa’s Crime Intelligence Unit. Anneli Botha holds a Magister Artium degree from Rand Afrikaans University in Political Studies (1998) and Philosophiae Doctor from the Department of Political Studies and Governance at the University of the Free State (2014). Her award-winning Ph.D. thesis was titled: “Radicalization to Commit Terrorism from a Political Socialization Perspective in Kenya and Uganda.” Additionally, she is a graduate of the University of Pretoria, Political Science (1991) and International Politics (1992).

Mahmut Cengiz is author of chapter 16. Dr. Cengiz is Assistant Professor and Research Faculty member with the Terrorism, Transnational Crime and Corruption Center (TraCCC) at
the Schar School of Policy and Government of George Mason University. He has international field experience, delivering capacity building and training assistance to international partners in the Middle East, Asia and Europe. He also worked on various research projects for the Brookings Institute, the European Union, and for U.S. government agencies. Mahmut Cengiz regularly publishes books, articles and op-eds on the Syrian conflict, terrorism, transnational crime, and corruption in the Middle East. His book, *The Illicit Economy in Turkey: How Criminals, Terrorists, and the Syrian Conflict Fuel Underground Economies* (2019), analyzes the role of criminals, money launderers, and corrupt politicians and discusses the involvement of ISIS and al-Qaeda-affiliated groups in underground economies. Mahmut Cengiz holds two Masters and two doctorate degrees. His graduate degrees in sociology were obtained at Turkish universities. He holds a Master’s from the American University School of International Service Program and a doctorate from the School of Public Policy program at George Mason University. Currently, he teaches Terrorism, American Security Policy and Narco-terrorism courses at George Mason University.

**Richard J. Chasdi** is author of chapter 32. He is a Professorial Lecturer, Department of Political Science, George Washington University. He is also an Adjunct Senior Fellow, International Center for Political Violence and Terrorism Research (ICPVTR) at the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, Singapore. Prior to that, Dr. Chasdi was a Professor of Management at Walsh College, Troy, Michigan. He received his B.A. in politics from Brandeis University in 1981, his M.A. in Political Science from Boston College in 1985, and his Ph.D. in Political Science from Purdue University in 1995. He has published four books on terrorism and counterterrorism, and several book chapters and refereed academic articles. Chasdi’s first book, *Serenade of Suffering: A Portrait of Middle East Terrorism, 1968-1993* (Lexington Books, 1999) received Choice magazine’s “Outstanding Academic Title” in the field of International Relations in 2000. Dr. Chasdi serves on the editorial boards of *Perspectives on Terrorism* and *Armed Forces & Society*. In 2017, Chasdi was a Fulbright Specialist at RSIS at Nanyang Technological University, working as a Visiting Fellow at the International Centre for Political Violence and Terrorism Research (ICPVTR). He has served as a news consultant for various radio and TV stations in the United States and abroad.

**John D. Colautti** co-author of chapter 31. He is a researcher and doctoral student in the School of Criminology and Justice Studies, University of Massachusetts, Lowell. He is also an Adjunct Professor at Fitchburg State University, an instructor with Crisis Systems Management, LLC, and an instructor with the Massachusetts Municipal Police Training Committee. He has over 30 years of probation, law enforcement and private security experience.

**Jessica Davis** is author of chapter 14. She is an international expert on terrorism and illicit financing. She began her career in intelligence analysis with the Canadian Military, then transitioned to a policy role at Global Affairs Canada before becoming a team leader with Canada’s financial intelligence unit, FINTRAC. Ms. Davis’s last role in government was as senior strategic analyst at CSIS where she was responsible for terrorism financing issues and managing the Indicators of Mobilization to Violence project. Ms. Davis is now the president and principal consultant with Insight Threat Intelligence, and works to bring evidence-based solutions to the private and public sectors to counter illicit financing and terrorism. Ms. Davis has published extensively, and is most recently the author of *Women in Modern Terrorism: From Liberations Wars to Global Terrorism and the Islamic State* (2017).

**Kenneth A. Duncan** is author of chapter 20. Dr. Duncan is a retired US Senior Foreign Service Officer. On September 5, 2001, he became Chairman of the Interagency Intelligence
Committee on Terrorism and its Community Counterterrorism Board. In this capacity he was responsible for providing formal warning of terrorist threats on behalf of the Intelligence Community to the highest levels of the Federal Government and for formulating and levying intelligence collection requirements on the Intelligence Community. Prior to his selection for this post by the Director of Central Intelligence, he was Charge d’Affairs, a.i. at the US Embassy in Haiti. He also served in the Department of State’s Bureau of Intelligence and Research (INR) as Director of the Office of Intelligence Coordination and as Deputy Department representative on the National Counterintelligence Policy Board. As such he was Senior Advisor to the Secretary of State for all matters involving counterintelligence and sensitive law enforcement activities. He also served as the analyst for Middle-Eastern terrorism in INR and taught courses on terrorism at Yale University and at the United States Coast Guard Academy. On retirement from the Foreign Service, he became Senior Adjunct Professor of Terrorism at the George C. Marshall European Center for Strategic Studies in Garmisch-Partenkirchen, Germany.

James J.F. Forest is co-author of chapter 31. He is a Professor in the School of Criminology and Justice Studies at the University of Massachusetts Lowell. From 2010 to 2019 he was also a Senior Fellow at the U.S. Joint Special Operations University. Currently, he is a Visiting Professor at the Fletcher School of Law and Diplomacy, Tufts University. Previously, Dr. Forest was Director of Terrorism Studies at the United States Military Academy. During his tenure at West Point (2001-2010) he directed a series of research initiatives and education programs for the Combating Terrorism Center at West Point (CTC), covering topics such as terrorist recruitment, training, and organizational knowledge transfer. Dr. Forest also served as an Assistant Dean at West Point. Prof. Forest has published 20 books and dozens of scholarly research articles and reports in this field, and is co-editor of the peer-reviewed scholarly journal Perspectives on Terrorism.

Ioannis Galatas is author of chapter 17. He is a retired Brigadier General in the Greek Army and as a military physician he specialized in Allergy and Clinical Immunology. Since 2001 he has been involved in CBRNE operations as planner and instructor and trained (including live agent training) in a number of countries abroad. During the 2004 Athens Olympic Games, he served as Commandant of the Olympic Hospital’s CBRN Response Unit. He holds an MSc. on “International Terrorism, Organized Crime and Global Security” (Coventry University, UK) and he is a Ph.D. candidate (Athens Medical School/ Forensics). His last assignment was as Head of the Dept. of Asymmetric Threats, J Mil Intel Service, HNDGS. Currently, he is the Editor-in-Chief of the online “C²BRNE Diary”; a Senior Research Associate at the Center for Security Studies, HMoI (Greece); a member of the Didactical Board of the University of Rome “Tor Vergata” for “International CBRNe Master” programs; a CBRN consultant, Emergency Department, Gemelli Policlinico, Catholic University of Sacred Heart, Rome (Italy); the Manager of the CBRN Knowledge Center, International CBNE Institute (Belgium), and a Senior CBRN Consultant at HotZone Solutions (The Netherlands).

Hans J. Giessmann is co-author of chapter 4. Between 2012 and 2019 Prof. Giessmann was Executive Director of the Berghof Foundation and Director of Berghof Conflict Research. Before joining Berghof in 2008, he was Deputy Director and Senior Researcher at the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH). His systematic research on terrorism began in 1995. At the beginning, his research focus was primarily on the challenges for countering terrorist violence whereas his main interest shifted later to provide technical support to actors willing to enter into peace negotiations in asymmetric armed conflicts, most recently in Afghanistan. From 2009 until 2014 he was a member of the Global Council on Terrorism to the World Economic Forum, and chaired the Council in 2011 and
2012. He graduated from the Humboldt University in Berlin in 1978 (Dipl.-Phil.) and holds doctorates in philosophy (1981) and in political science (1987). In the past, he has held guest professorships in the universities in Garden City (N.Y.), Wroclaw and Shanghai and visiting fellowships at EWI in New York and EU-ISS in Paris. As author, editor or co-editor he has published more than 40 books and about 400 research reports and articles, with numerous translations into more than ten languages. 

**Sajjan M. Gohel** is author of chapter 15. He has a multi-disciplinary background in global security issues. Dr. Gohel’s current research includes looking at the ideologies and doctrines that feeds international terrorism, the varying tactics and strategies of trans-national political violence, border security challenges, and the role new media play for strategic communications. As International Security Director for the London-based Asia-Pacific Foundation, a policy assessment think-tank monitoring emerging geopolitical threats, Sajjan acts in a consultancy role for law enforcement agencies, foreign ministries and defence departments, multilateral organizations, universities, NGOs and the international media. Sajjan Gohel has also provided in-depth reports on security issues to the European Union, UNHCR, NATO, OSCE and INTERPOL. Sajjan’s research is case-study driven and he has fieldwork experience in 23 countries. Sajjan has provided expert witness testimony to numerous political standing committees on the evolving challenges and threats in Afghanistan-Pakistan, North Africa and the Middle East. In his role as Senior Advisor to the Partnership for Peace Consortium’s Combating Terrorism Working Group (CTWG), he heads its programme development on countering violent extremism. The CTWG is a collaborative research project investigating current transnational security threats and comprises of members from over 30 countries and multilateral organizations. Sajjan received his BA (Hons) in Politics from Queen Mary, University of London. He also holds both a Master’s degree in Comparative Politics and a PhD in International History from the London School of Economics & Political Science (LSE) entitled, “Insurrection of the Ideologues: The Evolution of Egyptian Islamist Radical Ideological Thought from Hasan al-Banna to Ayman al-Zawahiri.”

**Joseph Gyte** is co-author of chapter 12. He is the Senior Program Associate within the Capacity Building Department at Hedayah, the International Center of Excellence for Countering Violent Extremism in Abu Dhabi. Joseph Gyte supports the curriculum development, implementation and evaluation of capacity building programs, and leads a program for psychologists and social workers to support families affected by violent extremism. Prior to joining Hedayah, Joseph Gyte worked as a Terrorism Prevention Program Consultant at the United Nations Office on Drugs and Crime (UNODC), Regional Office for Southeast Asia and the Pacific. In this position, he acted as focal point for the planning and implementation of capacity building activities related to Counter Terrorism in Indonesia, Myanmar and the Philippines. He also contributed technical inputs towards the development of a National Action Plan to Prevent Violent Extremism in a Southeast Asian country, and produced multiple training manuals, handbooks, publications and Op-Eds, on behalf of UNODC. Joseph Gyte has also worked in the Office of the EU Counter-Terrorism Coordinator in Brussels, where he was directly involved in the EU’s development of policy responses to the evolving phenomena of foreign terrorist fighters and violent extremism. Joseph Gyte’s educational background includes a Master’s degree in Terrorism Studies from St. Andrews University and a Bachelor’s degree in Psychology from Cardiff University.

**Gary Hill** is author of chapter 8. He is the chief executive officer of CEGA Services in Lincoln, Nebraska (USA) and president of Contact Center, Inc., a private, nonprofit, international information and referral clearinghouse working in the areas of human services, criminal justice and illiteracy. Hill has been working in the field of corrections since 1964 and is the recipient
of the American Correctional Association’s highest award. On special assignment to United Nations organizations, he has drafted more than forty training manuals in support of formal training programs for prison workers. Gary Hill is the Staff Training and Development Director of the International Corrections and Prisons Association (ICPA) and works with several Institutes of the United Nations Crime Prevention and Criminal Justice Program. He served on the United Nations Committee of Experts which prepared the update of the United Nations Standards for the Treatment of Offenders (the Mandela Rules) and the development of the standards for female offenders (the Bangkok Rules). For the Best Practices Unit of the United Nations Office of Peacekeeping Operations, Gary Hill reviewed the corrections activities associated with UN Peacekeeping and prepared a “Lessons Learned” document and a guidebook for use in future missions. He serves as an expert on three Council of Europe projects dealing with prison radicalization.

Shashi Jayakumar is author of chapter 29. Dr. Jayakumar is Head, Centre of Excellence for National Security (CENS) and Executive Coordinator, Future Issues and Technology at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. Shashi Jayakumar was a member of the Singapore Administrative Service from 2002-2017. During this time, he was posted to various ministries, including the Ministries of Defence, Manpower, Information and the Arts, and Community Development, Youth and Sports. From August 2011-July 2014 he was a Senior Visiting Research Fellow at the Lee Kuan Yew School of Public Policy. His research interests include extremism, social resilience, cyber issues, and homeland defense.

Brian Michael Jenkins is author of chapter 26. He holds academic degrees from the University of California at Los Angeles. He also studied at the University of Guanajuato, Mexico, and at the University of San Carlos, Guatemala. Commissioned in the Army at the age of 19, Mr. Jenkins became a paratrooper and captain in the Green Berets. He served in the 7th Special Forces Group in the Dominican Republic and later as a member of the 5th Special Forces Group in Vietnam (1966–1967). He returned to Vietnam in 1968 to serve as a member of the Long Range Planning Task Group. In 1989, Mr. Jenkins served as an advisor to the national commission established to review terrorist threats following the bombing of Pan Am 103. Following the 1993 bombing of the World Trade Center, he served as a member of the team assembled to review threats and develop new security measures. In 1996, President Clinton appointed Mr. Jenkins to the White House Commission on Aviation Safety and Security. From 1999 to 2000, he served as an advisor to the National Commission on Terrorism. Mr. Jenkins is the Senior Adviser to the President of the RAND Corporation and also the Director of the National Transportation Security Center at the Mineta Transportation Institute. B.M. Jenkins is the author of International Terrorism: A New Mode of Conflict; the editor and co-author of Terrorism and Personal Protection; the co-editor and co-author of Aviation Terrorism and Security. His other books include Unconquerable Nation and Will Terrorists Go Nuclear?

Asad Ullah Khan is co-author of chapter 10. He is a Senior Research Fellow at the Center for Aerospace and Security Studies (CASS). Until recently, he was a Research Fellow for Counter-Terrorism and Countering Violent Extremism at the Institute of Strategic Studies Islamabad. Asad Ullah Khan’s area of research is national security and counter-terrorism. He represented Pakistan on many national and international forums on the subject matter. He is the author of numerous research articles, book chapters and opinion articles in journals, books and magazines in the domain of countering violent extremism. Mr. Khan has recently represented Pakistan at a Colombo Defence seminar in Sri Lanka and shared his research work on the forum.
**Nina Käsehage** is author of chapter 11. Dr. Käsehage is a Senior Lecturer at the Department of Religious Studies and Intercultural Theology, University of Rostock, Germany. Currently Nina Käsehage is preparing a ‘Habilitation’ on the religious socialization of children who were raised by the Islamic State. In 2017, she completed her doctoral dissertation ‘The current Salafi Scene in Germany - Preachers and Adherents’ (‘Die gegenwärtige salafistische Szene in Deutschland- Prediger und Anhänger’) at the Department of Religious Studies of Georg-August-University, Göttingen. Her thesis was based on more than one hundred in-depth interviews with Salafi preachers and members of groups such as Milatu Ibrahim (MI). More recently, she conducted 60 interviews with female Jihadists in nine European countries for her forthcoming book ‘Women in Jihad’ (‘Frauen im Dschihad’). She is a member of the German Association of Religious Studies (DVRW), the Commission for Diversity and Equality of the University of Rostock and the European Experts Network on Terrorism Issues (EENeT). She is a member of the think-tank Cologne Forum for Domestic and Security Policy (KFBIS). In addition, she is the founding member of the scientific advisory board RadiPräv, a Göttingen-based organization for the prevention of religiously motivated radicalization. In addition, she offers consulting services in the field of Salafism, Jihadism, Takfirism and on religious radicalization.

**Susanne Martin** is author of chapter 25. Dr. Martin is an Associate Professor of Political Science and Director of the International Affairs Program at the University of Nevada, Reno. In addition to her work on prevention, Susanne Martin’s work on suicide attacks also includes studies of the history of suicide tactics in warfare and analyses of changes in suicide tactics. Susanne Martin also works on themes relating to political violence and warfare, more generally, with a focus on the groups that engage in violent activities, the conditions under which groups use violent versus nonviolent tactics, and the types of groups that are more likely to abandon violence. Insurgent groups and terrorist groups are the focus of much of her work, along with the political parties with which some of these groups have affiliations. Professor Martin is co-author (with Leonard Weinberg) of The Role of Terrorism in Twenty-first-century Warfare (Manchester University Press, 2016). In this work the authors explore patterns in the timing of terrorism within wider-scale warfare. Susanne Martin is also author of “Dilemmas of ‘Going Legit’: Why Should Violent Groups Engage in or Avoid Electoral Politics?” (2014), published in the journal Behavioral Sciences of Terrorism and Political Aggression. She is also a student of language, with formal training in German, Spanish, Serbian, Bosnian, Croatian, French, and Czech. Professor Martin earned her doctorate in Government at the University of Texas at Austin.

**Clark McCauley** is author of chapter 6. He is Research Professor of Psychology at Bryn Mawr College. His research interests include stereotypes, group dynamics, and the psychological foundations of ethnic conflict and genocide. He is co-author of Why Not Kill Them All? The Logic and Prevention of Mass Political Murder (2006), co-author of Friction: How Radicalization Happens to Them and Us (2011, second edition 2017), co-author of The Marvel of Martyrdom: The Power of Self-Sacrifice in a Selfish World (2018). Dr. McCauley is founding editor emeritus of the journal Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide. He is also a lead investigator with the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland.

**David McIlhatton** is co-author of chapter 23. He is a Professor of Protective Security and Resilience, and the Director of the Institute for Peace and Security at Coventry University. He has published widely on counter-terrorism, and is on a number of editorial boards of international peer-review journals and reviews for multiple terrorism journals. His research portfolio includes projects with a value of over £ 17 million in security and business related
research areas internationally. He has been awarded with numerous international prizes for research excellence, and was nominated to the Royal Society of the Arts as a result of his work in human security. He is also a Visiting Scholar at the University of Central Oklahoma.

**Juan Merizalde** is co-author of chapter 31. He is a researcher and doctoral student in the School of Criminology and Justice Studies, University of Massachusetts, Lowell. His research interests include asymmetric warfare, the private defense sector, counter-terrorism policy, and community resilience. Previously, Juan served in the U.S. Air Force where he was deployed in Operation Enduring Freedom and Operation Iraqi Freedom.

**Rachel Monaghan** is co-author of chapter 23. Dr. Monaghan is Professor of Peace and Conflict at the Centre for Trust, Peace and Social Relations at Coventry University. Her research interests focus on political violence, informal justice, single-issue terrorism, counter-terrorism and crime and insecurity. She has been researching animal rights extremism for 30 years and has published articles on the subject in *Terrorism and Political Violence* and *Studies in Conflict & Terrorism*. She is Co-Editor of the journal *Behavioral Sciences of Terrorism & Political Aggression* and is currently the President of the Society for Terrorism Research.

**Shannon Nash** is author of chapter 30. Dr. Nash is the Postdoctoral Network Manager of the North American and Arctic Defence and Security Network (NAADSN). This collaborative network provides timely, relevant, and reliable expert advice on North American and Arctic defence and security topics. Shannon Nash is a Research Fellow at Trent University with NAADSN and has ongoing projects at the University of Waterloo, examining education and training in national security and counter-terrorism in Canada and exploring how the “terrorism” label is informed and applied to violent attacks in Canada. She received her Ph.D. in History from the University of Toronto with a focus on 20th century American history, terrorism, and international relations. She studies past and present terrorist threats and attacks as well as Canadian, American, and international defence, security and counterterrorism policies. Shannon’s doctoral thesis focused on the reality of al Qaeda espionage methodology and how the idea of a sleeper agent was perceived and adapted to fit the terrorist threat posed by al Qaeda from the 1990s onwards.

**Annelies Pauwels** is author of chapter 22. She is a Research Fellow at the Flemish Peace Institute in Brussels, where she focuses on terrorism and violent extremism. Prior to that she conducted research on crime prevention and criminal justice for various international organizations, including the EU Institute for Security Studies (EUISS), the UN Office on Drugs and Crime (UNODC), and the UN Interregional Crime and Justice Research Institute (UNICRI). Her previous research projects have focused on various aspects of international security, including jihadist and far-right terrorism, migration, and organized crime. Annelies Pauwels holds an LLM in International Criminal Law and an MA in Intercultural Mediation, with a specialization in Arabic and Russian. She is fluent in English, French, Italian, and Dutch and has a working knowledge of Spanish, Arabic, and Russian.

**Tom Parker** is author of chapter 34. He was until recently the Chief of Party of a European Union project providing assistance to the Office of the National Security Adviser in Baghdad, Iraq and is currently providing advice to the Nigerian government. Tom Parker has previously served as an adviser on human rights and counter-terrorism to the United Nations Counter-Terrorism Implementation Task Force (CTITF) and was one of the principal authors of the UN’s Preventing Violent Extremism Plan of Action. He has also worked as Policy Director for Terrorism, Counterterrorism and Human Rights for Amnesty International USA, as a war crimes investigator for the United Nations International Criminal Tribunal for the former
Yugoslavia (ICTY) working in the field in Bosnia and Kosovo, and as an Intelligence Officer in the British Security Service (MI5). He has taught undergraduate and postgraduate courses on international terrorism in Yale University’s Residential College Seminar Program, Bard College’s Globalization and International Affairs Program, and the US National Defense University at Fort Bragg. He is the author of *Avoiding the Terrorist Trap: Why Respecting Human Rights is the Key to Defeating Terrorism* (2019).

**Marie Robin** is the author of chapter 33. She is a PhD candidate affiliated with the Center for War Studies at the University of Southern Denmark, and the Centre Thucydide at Université Paris 2 Panthéon-Assas. Her dissertation proposes a conceptualization of the role of revenge in International Relations by analyzing the revenge narratives of the Islamic State, Al Qaeda, and Boko Haram. For her dissertation, Marie received funding from DGRIS/IRSEM. She presented her research at ISA Toronto, EISS Paris, as well as various national conferences. Marie taught courses of Ethics and of International Relations at Sciences Po, at the Université de Lille, and at the University of Southern Denmark. She also organized the first edition of the Graduate Conference of the War Studies Network in January 2020. In addition to her PhD, she works as a research assistant and translator for various academic publications and centers.

**Alexander von Rosenbach** is author of the Foreword. Currently he serves as Interim Director of the International Centre for Counter-Terrorism (ICCT). Before joining ICCT, he worked as a Senior Technology Analyst & Project Manager for a New York City startup, managing enterprise-level business processes and technology solutions. He also worked for five years at Jane’s, a London-based open-source intelligence provider to militaries, governments, intelligence agencies and industry. There, he led a team of analysts and researchers assessing military capabilities and threats around the world. As ICCT’s Interim Director, Alexander von Rosenbach brings more than 10 years of commercial and security experience to bear on ICCT’s content, strategy, finance and organizational design. Prior to his appointment as Interim Director, Alexander held the position of Operations Manager of ICCT. He holds a Master’s degree in International History from the London School of Economics and a Bachelor’s degree in Political Science from the University of British Columbia.

**Thomas Koruth Samuel** is author of chapter 7. He is a consultant with the United Nations Office on Drugs and Crime (UNODC) and the United Nations Development Programme (UNDP). His main areas of interest include Preventing and Countering Violent Extremism (PCVE), countering terrorist narratives, the role of education in Countering Violent Extremism (CVE) and youth radicalization. He started off as a volunteer Health Officer for World Vision East Timor in 2003. Thomas Samuel has an Honours degree in Biomedical Technology, a Master’s degree in Strategic and Defence Studies and is at present pursuing his Ph.D., focusing on the role of the quest for personal significance in motivating terrorism among Malaysian youths. He has been a Senior Fellow with the International Centre of Excellence for Countering Violent Extremism (Hedayah Centre) since 2014. In 2018, he was appointed as a member of the Commonwealth CVE Cadre of Experts.

**Andreas Schädel** is co-author of chapter 4. He is a Research Fellow at the Berghof Foundation in Germany and Advisor for Design, Monitoring and Evaluation in peacebuilding and conflict transformation projects. He has worked for the disarmament section at the Swiss Mission to the United Nations in Geneva and in various positions in the academic and financial sectors. Andreas Schädel earned his Ph.D. from the Chair of International Conflict Research at ETH Zürich with a dissertation on the role of reputation in separatist conflicts. He holds an MA in International and Comparative Studies from ETH Zürich and received his BA in Political
Science and Economics after studying at the University of Zürich and at the Institut d’Études Politiques de Bordeaux.

**Joshua Sinai** is author of chapter 21. Dr. Sinai is a Professor of Practice in Counterterrorism Studies at Capitol Technology University, in Laurel, Maryland, USA. He also teaches a graduate-level distance learning course on “Global Terrorism” at Southern New Hampshire University’s Criminal Justice Department. He has more than 30 years of professional experience in terrorism and counterterrorism studies in the U.S. Government, academia, and the private sector. He specializes in analyzing and mitigating what is termed “active threats”: terrorism, active shooters, workplace violence, and “insiders”. A widely published author, his publications include “Active Shooter: A Handbook on Prevention” (ASIS International, May 2016, 2nd edition); a chapter on “The United States of America’s Domestic Counterterrorism Since 9/11,” in: Andrew Silke (ed.), *Routledge Handbook of Terrorism and Counterterrorism* (Routledge, 2018); and a chapter on “Israel and Combating Terrorism: Assessing the Effectiveness of Netanyahu’s Combating Terrorism Strategy”, in Robert O. Freedman (ed.), *Israel Under Netanyahu: Domestic Politics and Foreign Policy* (Routledge, 2020). As a veteran book reviewer, he serves as Book Reviews Editor of the online journal *Perspectives on Terrorism*, for which he also writes the “Counterterrorism Bookshelf” review column. He earned his Master’s degree and PhD from Columbia University in Political Science.

**Ishaansh Singh** is the compiler of the general bibliography of the *Handbook of Terrorism Prevention and Preparedness*. Since 2018 he is a student at the Symbiosis School for Liberal Arts, Pune. His major and minor fields of specialization are International Relations and Peace and Conflict Studies. Additionally, he served as an intern for the Terrorism Research Initiative, Vienna. He is currently preparing a thesis on the factors that led to Brexit.

**Barbara Sude** is author of chapter 9. Dr. Sude has served more than 30 years with the U.S. Government, where she specialized in analysis of terrorism, political Islam, Sub-Saharan Africa, and the Middle East. As an adjunct researcher and former senior political scientist at the RAND Corporation, Barbara Sude most recently focused on counterterrorism, refugees, and asymmetric warfare. She has given several public presentations and media interviews on counterterrorism issues and is the lead author of *Lessening the Risk of Refugee Radicalization: Lessons for the Middle East from Past Crises* (RAND Corporation, 2015) and co-author of *Knowing the Enemy: Understanding the Islamic State and Principles for Defeating It* (RAND 2017) and *An Economic Analysis of the Financial Records of al-Qa’ida in Iraq* (RAND Corporation, 2010). She received her BS in Arabic from Georgetown University and her Ph.D. in Near Eastern Studies from Princeton University.

**Branislav Todorovic** is co-author of chapter 19. Dr. Todorovic is a member of the Institute for National and International Security (INIS), Serbia, and a Senior Research Associate in NTUA - National Technical University of Athens and AUA - Agricultural University of Athens, Greece. He also cooperates since 1989 with MASBG - Faculty of Mechanical Engineering, University of Belgrade, Serbia. He is a full member of the Technical Chamber of Greece (TEE) and the Technical Chamber of Serbia. Branislav Todorovic has participated in many commercial and R&D projects, and produced international conference papers. His background covers 30 years of work in environmental sciences, energy and water topics, Critical Infrastructure Protection (CIP), cyber security and IT/ICT, especially GIS, CAD, programming & software development, 3D modelling, databases, etc. He has worked in multidisciplinary projects related to capacity building, public participation, energy and water resources management, renewable resources, modelling of processes, Decision Support Systems (DSS), expert systems, and complex designs.
Darko Trifunovic is co-author of chapter 19. Dr. Trifunovic is a Senior Research Fellow and lecturer at the Faculty of Security Studies of the University of Belgrade and a Senior Adviser at the Research Institute for European and American Studies in Athens, Greece. He is also a guest professor at FUDAN University – Center of American Studies, Shanghai, China. Dr. Trifunovic is a specialist in Security Studies, Intelligence & Counter Intelligence Studies as well as Counter-Terrorism, National and International Security Studies. He is a former diplomat (First Secretary of the Foreign Service of BiH at the UN). Dr. Trifunovic is the representative for Serbia and Montenegro in the International Strategic Studies Association (ISSA). He is a member of the Advisory Board of the Institute of Transnational Studies, Munich, Germany. Dr Trifunovic is regular speaker at the International Counter Terrorism Institute, Tel Aviv, Israel, and one of the founding Members of the International Counter Terrorism Academic Community (ICTAC). He has published a number of academic books, papers and articles.

Ifrah Waqar is co-author of chapter 10. Her academic career is in International Relations. She has extensive experience of working with various national and international organizations over the past five years on issues ranging from terrorism, countering violent extremism and radicalism, foreign policy, as well as strategic and nuclear issues. She has been developing and working with the Centre for Pakistan and Gulf Studies’ CVE project, SALAM, which deals with innovative methods to address radical extremism and countering violent extremism in Pakistan. She was Project Manager for Countering Violent Extremism, under the premises of the Centre’s flagship project SALAM. In 2017, she visited the Kingdom of Saudi Arabia at the invitation of a Saudi think-tank. Ms. Waqar has also served as the Special Assistant to the Convener of Pakistan-Kingdom of Saudi Arabia Senate Friendship Group, Senator Sehar Kamran, from May 2016 till March 2018.

Rob de Wijk is author of chapter 5. Prof. de Wijk is founder of The Hague Centre for Strategic Studies (HCSS) and Professor of International Relations and Security at the Faculty Governance and Global Affairs (ISGA), Leiden University. He studied Contemporary History and International Relations at Groningen University, and wrote his Ph.D. dissertation on NATO’s ‘Flexibility in Response’ strategy at the Political Science Department of Leiden University. Rob de Wijk started his career in 1977 as a freelance journalist and later became head of the Defense Concepts Department of the Dutch Ministry of Defense, head of the Security Studies at the Clingendael Institute, and Professor of International Relations at the Royal Netherlands Military Academy. He wrote extensively on security affairs, including The Art of Military Coercion (Amsterdam: AUP, 2004) and Power Politics (Amsterdam: AUP, 2015).

Ahmet S. Yayla is author of chapter 13. Dr. Yayla is Assistant Professor at De Sales University’s Homeland Security Department. He is also a Research Fellow at the Program on Extremism at George Washington University and a faculty member at Georgetown University’s School of Continuing Studies. Ahmet Yayla served previously as a Full Professor and Chair of the Department of Sociology at Harran University in Turkey. He is a 20-year veteran of the Counterterrorism and Operations Department in the Turkish National Police and served as the Chief of Counterterrorism in Sanliurfa between 2010 and 2013. He is an experienced practitioner in counterterrorism and has advised senior government officials around the world during his career in law enforcement and academia. Ahmed Yayla has published both scholarly works and written or co-authored numerous articles on mainstream news platforms related to counter-terrorism and homeland security.
Sara Zeiger is co-author of chapter 12. Sara Zeiger is the Program Manager for the Department of Research and Analysis at Hedayah, the International Center of Excellence for Countering Violent Extremism in Abu Dhabi. Sara Zeiger supports the Director in managing the Department’s resources and programs, including the Counter-narrative Library, Hedayah’s non-resident Fellowship Program and Hedayah’s annual International CVE Research Conference. Sara was also the lead content developer for Hedayah’s App, MASAR, that provides practical guidance on MM&E for CVE. She has also been a co-Director for a NATO Science for Peace and Security (SPS) grant on enhancing the role of women in international CVE efforts. In addition to her duties in the Department of Research and Analysis, she was also Hedayah’s liaison with the Global Counterterrorism Forum (GCTF) to support the development and drafting of their framework document, the Abu Dhabi Memorandum on Good Practices for Education and CVE and the follow-up Action Plan. Sara Zeiger is currently a Non-Resident Fellow in International Relations and Counter-Terrorism for TRENDS Research & Advisory. Prior to joining Hedayah, Sara worked as a Research Assistant at the Center for Middle Eastern Studies at Harvard University. She also served as a Head Teaching Fellow for the Harvard Extension School where she taught courses on anthropology in the Gulf, politics in the Middle East, and Islam in the West. Sara Zeiger holds a Master’s in International Relations and Religion (concentrations: Security Studies and Islam) from Boston University, and graduated as valedictorian with a B.A. in Psychology and Religion from Ohio Northern University.
Foreword

More than a year ago, Prof. em. Alex Schmid approached the International Centre for Counter-Terrorism - the Hague (ICCT) with a proposal. He was working on another handbook on terrorism, this time specifically focused on prevention and preparedness. A formidable line-up of academic scholars and leading edge practitioners from around the world had already agreed to submit chapters. He was visiting The Hague inquiring whether ICCT would consider the handbook for publication.

Naturally, my colleagues and I jumped at the opportunity. At ICCT, we are honoured to count Prof. Schmid as one of our longest-serving Research Fellows. His research contributions have in many respects powered the growth and success of the ICCT Journal, serving as a beacon to all those seeking to understand the phenomenon of terrorism. His seminal 2013 paper entitled “Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review” has become essential reading on countless counter-terrorism academic curricula, and is the most well referenced research contribution ICCT has ever produced.

I asked Prof. Schmid, “What made you write and compile this new Handbook?” His answer,

“It had been on my mind for more than twenty years – ever since I became Officer-in-Charge of the Terrorism Prevention Branch at UNODC in 1999. However, I never had the time and I also hoped that somebody else would bring together all that we know about prevention. But when nobody else did it, I felt that I had to do it myself. It was like a burden I carried with me during all those years. Now I feel a great sense of relief.”

The second question I had was, “Why bring your handbook to ICCT rather than a traditional publishing house?” I remember the reply vividly. Prof. Schmid said that he had considered producing his handbook through the normal publishing channels and had offers from two major publishers. However, he feared choosing that route would result in a handbook too expensive for general use and therefore one destined for dusty bookshelves in university libraries. He had a different vision for his work and that of his contributing authors.

Together, we decided that the Handbook of Terrorism Prevention and Preparedness, as it is now titled, would sit better with ICCT because of our institutional commitment to make counter-terrorism research freely available. Extending beyond our journal, this handbook is the first official publication of ICCT as an independent press - ICCT Press.

The ICCT Journal is at the core of the institute’s knowledge-sharing activities and is the most visible aspect of ICCT’s work to inform the public debate on countering and preventing violent extremism and terrorism. Its open access format means that its publications can be read, debated and cited in any context, from first-year university student papers to European Parliamentary debates and United Nations Counter-Terrorism working groups.

ICCT takes great pride in our highly professional editorial team and large global readership, but we also knew from the outset that the comprehensive nature of the Handbook – running upwards of 500,000 words across 35 in-depth chapters (six by Prof. Schmid himself) – would push our editorial practices to their limit. As a result, we decided to publish it in five parts, ultimately bringing it all together in 2021 in a single online volume of over 1,250 pages. Along the way, we will host a series of online events, giving our global community an opportunity to engage directly with the Handbook’s prestigious authors.

It is our shared ambition that the Handbook of Terrorism Prevention and Preparedness – produced by ICCT Press and hosted freely on the ICCT website – becomes an authoritative resource on many aspects of anticipatory counter-terrorism. The strength of its contribution to the field is unarguable: starting with first principles and an extensive analysis of lessons for
terrorism prevention that can be drawn from related fields, the handbook then follows the full arc of the terrorist threat – from prevention of radicalization to prevention of preparatory acts and preparedness for mitigating the consequences of attacks – shedding new light on how to strengthen our institutions, our infrastructure and our societies to better counter the threat of terrorism.

I am sure that the readers of these chapters will find it a comprehensive analysis of the challenges facing today’s policy-makers and counter-terrorism professionals, and a vital and enduring ready reference on terrorism prevention and preparedness.

Alexander von Rosenbach
Interim Director, ICCT

The Hague, 1 July 2021
Acknowledgements

With the publication of this *Handbook of Terrorism Prevention and Preparedness*, a burden falls from the shoulders of the editor as this project has been on his mind for many years and it is good to see its completion. It rests me as editor to thank all the contributors for their work: I am truly grateful to all of you! I also wish to thank Renske van der Veer, Alexander von Rosenbach, Joana Cook, Ruth Heylin, Anna-Maria Andreeva, Maarten Visser, Antoinette van den Berg, Teo Kai Xiang and Charlie van Mieghem at ICCT for facilitating the production of this book. Last but not least, I am grateful to my wife, Dr. Shantu Watt, who stood by me in troubling times.

Alex P. Schmid

The Hague, July 2021
Chapter 1

Introduction: Purpose and Organization of the Handbook

Alex P. Schmid

The idea for this Handbook of Terrorism Prevention and Preparedness goes back twenty years. I first had the desire to put together such a Handbook two decades ago when, between 1999 and 2005, I was Officer-in-Charge of the Terrorism Prevention Branch (TPB) of the UN Office on Drugs and Crime (UNODC) in Vienna, Austria. In the wake of the events of 9/11, those were very busy days. However, not only was there not enough time to write or assemble such a volume, I did not have a mandate from the UN Crime Commission, nor were there any resources made available from UN member states to do so. Since then much has changed - but neither TPB nor any of the other UN Counter-Terrorism agencies and branches has produced a work like the present one.

Once I retired from the United Nations, I no longer had to wait for an official mandate and I finally had enough time to produce this Handbook with the help of friends and colleagues who were prepared to contribute a chapter. I received technical support for producing this volume from the International Centre for Counter-Terrorism - The Hague (ICCT) of which I am, since 2012, a Research Fellow.

The choice for an online publication was the result of the following consideration. A volume with more than 1,000 pages, marketed by a commercial publisher, would have been prohibitively expensive for the average reader and would have placed it well beyond the budget of some of the people who might profit most from it. The decision to make this Handbook freely available online was supported by the volume’s contributors who all felt that this was the right thing to do to achieve maximum distribution with no loss of time. I am deeply thankful to them as well as to the staff of ICCT which provided the necessary support.

The need for a Handbook of Terrorism Prevention and Preparedness needs little explanation in the light of the fact that the dominant approach of counterterrorism, based largely on heavy-handed military action, has been such a failure - especially in the Middle East. The traditional military instrument of deterrence has not worked against enemies who have, in most cases, no fixed territorial basis while claiming to love death more than life. The decapitation of terrorist organizations by killing their leaders in drone strikes has created martyrs rather than broken their organization’s will to fight. The collateral damage of military strikes has often turned family members, friends and other witnesses near and far into avengers. For many societies, the “cure” of militarized counterterrorism has been worse than the “disease” of terrorism.

The following facts substantiate this claim. Since 9/11, much of counterterrorism has been counter-productive. Al-Qaeda numbered only about 400 fighters in Afghanistan when 19 of them killed nearly 3,000 civilians from more than sixty countries on September 11, 2001, in the US. Today there are, next to Al-Qaeda, about one hundred other Islamist extremist groups active in nearly 70 countries worldwide, killing more than 120,000 people in the last few years alone.¹ Al-Qaeda and its affiliates now have an estimated 40,000 fighters. Altogether there are
some 230,000 active jihadists in our midst – not counting other religious as well as right-wing and other secular terrorists.

The US alone conducted military counterterrorism missions in 80 countries at a cost which has conservatively been estimated at US $2 trillion. The price paid by civilians in the ‘Global War on Terror’ (GWOT) has been staggering – in the post-9/11 wars an estimated 43,074 civilians died in Afghanistan, 23,924 in Pakistan, between 184,382 and 207,156 in Iraq, 49,591 in Syria, 12,000 in Yemen – altogether between 312,971 and 335,745 civilians or one hundred times more civilians than had perished in the 9/11 attacks. Add to this the members of national military and police forces in Afghanistan, Pakistan, Iraq, Syria and Yemen who lost between 173,073 and 335,745 men and women in uniform. Worldwide, between 770,000 and 801,000 human beings have died in the post-9/11 wars. This total estimate includes civilian deaths – some 312,000 or more – as well as dead terrorists (more than 250,000). In addition, an estimated 37 million people have been internally or externally displaced as a result of the wars the US military fought post-9/11. Given the fact that the counterterrorism efforts of the last two decades have taken such a heavy human toll and that victory is not in sight, it is high time to rethink the way terrorism should be countered. By focussing on prevention, this Handbook seeks to stimulate such rethinking.

The editor has invited nearly forty diverse scholars and (former) counterterrorism practitioners to share their insights with the readers of this volume. Some of the contributors are ‘old hands’ with decades of experience. Others are promising newcomers to the field. Most of the chapters have been written by single authors, but a few chapters have two or even three (co-) authors. 15 of the 43 contributors to this Handbook are women. While the majority of the authors are from Europe or North America, there are also more than a handful from Asia, the Middle East and Africa. The biographies of the contributors can be found at the end of each chapter.

The Handbook is structured into five parts, comprising 32 chapters, next to the two introductory chapters and a concluding chapter by the editor followed by a comprehensive bibliography as follows:

- Part I: Lessons for Terrorism Prevention from the Literature in Related Fields (4 chapters);
- Part II: Prevention of Radicalization (6 chapters);
- Part III: Prevention of Preparatory Acts (7 chapters);
- Part IV: Prevention of, and Preparedness for, Terrorist Attacks (10 chapters);
- Part V: Preparedness and Consequence Management (5 chapters).

The idea of combining prevention with preparedness requires little explanation. Preparedness contributes to prevention and, should prevention fail, preparedness reduces harm and facilitates better crisis- and consequence-management. The relationship between the two is fleshed out in more detail by the editor of this Handbook in chapter 2.

What follows here is a brief preview of the content of each of the following chapters.

Chapter 2: “Terrorism Prevention: Conceptual Issues (Definitions, Typologies and Theories)” has been written by Alex P. Schmid, the editor of the Handbook. Here the key concepts are explored, including the differences between terrorism prevention, prevention of radicalization and prevention of extremism – concepts with admittedly fuzzy borders. Prevention itself is by no means an un-problematical concept: while everyone agrees that prevention is generally a good thing when it comes to take precautionary measures against harmful phenomena and ominous developments, it is often less than clear where and when to apply which instruments and measures to achieve a non-event - the one prevented. The author introduces a distinction between upstream-, midstream- and downstream-terrorism prevention and outlines which type of measures ought to be considered in each of these phases as terrorism emerges and evolves. The conceptual and theoretical tools developed in the second chapter
have been offered to the other contributors of this \textit{Handbook} for consideration before they embarked on writing their chapters.

\textbf{Preview of the Five Parts and their Chapters}

\textit{PART I: Lessons for Terrorism Prevention from the Literature in Related Fields}

Since terrorism prevention is clearly lagging behind the study of prevention in some other, but related, research fields, Part I explores what can be learned from crime prevention, conflict prevention as well as from counterinsurgency studies and the genocide prevention literature.

Chapter 3 opens with a contribution by Kelly A. Berkell (Senior Research Fellow at the Center on Terrorism at John Jay College of Criminal Justice, New York), titled “A Criminological Approach to Preventing Terrorism: Situational Crime Prevention and the Crime Prevention Literature.” The author explores what “lessons learned” from crime prevention can teach us for the prevention of terrorism by introducing models and foundational concepts in crime prevention, with a focus on situational crime prevention and its theoretical underpinnings. In the field of terrorism studies, the political character of terrorism has often overshadowed its criminal nature but a crime remains a crime whether it is political or not. As the saying goes, opportunities not only make thieves, but can also make terrorists. Smart changes in environmental parameters, the author argues, can not only reduce ordinary crime hotspots but are also helpful against extraordinary terrorist acts.

Chapter 4 by Andreas Schädel (Research Fellow at the Berghof Foundation) and Hans J. Giessmann (Director Emeritus of the Berghof Foundation) is titled “De-Exceptionalizing the Terrorist Phenomenon: Lessons and Concepts from Conflict Prevention and Transformation.” It argues that terrorism is not as extraordinary as many of those think who argue that one should never shake hands with terrorist murderers. At the end of the day, most terrorist campaigns have been brought to a close not by superior law enforcement tactics or by military victories, but by secret negotiations. Terrorism is often part of a wider conflict and the instruments of conflict resolution should, the authors argue, be applied. Conflict prevention can also be a form of terrorism prevention, and while not all conflicts can be prevented there are opportunities for conflict transformation that should be explored.

Chapter 5 by Rob de Wijk (Founder of The Hague Centre for Strategic Studies [HCSS]) is titled “Contributions from the Military Counter-insurgency Literature for the Prevention of Terrorism.” The author notes that counter-insurgency (COIN) operations and counter terrorist operations, while sometimes overlapping, differ in important ways. COIN operations require a “hearts and minds” approach to win the trust of the people while counterterrorism operations, directed against small groups of clandestine actors, require search, arrest and neutralization tactics that should not inconvenience the general public too much. The author discusses the lessons that can be learned from various counterinsurgency operations for counterterrorist campaigns and explores the role of deterrence by denial and deterrence by punishment and their respective places in COIN and counterterrorism operations.

Chapter 6 by Clark McCauley (Research Professor of Psychology at Bryn Mawr College) is titled “‘Killing Them to Save Us:’ Lessons from Politicide for Preventing and Countering Terrorism.” While both terrorism and genocide involve the one-sided killing of unarmed civilians (though on a different scale), the two extremes of violence are rarely discussed together. This is exactly what the author – the founder of the journal \textit{Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide} - does. He stresses the importance of studying both sides in a conflict dyad when it comes to exploring the early phases of a conflict when prevention is still a possibility. The author also calls for an acknowledgment of the threats and grievances as perceived by both sides.
PART II: Prevention of Radicalization

Since nobody is born a terrorist, socialisation of an individual or group to accepting this form of one-sided killing of unarmed people, and mobilisation of an individual or group to actually engaging in murdering civilians (usually complete strangers), are required for most acts and campaigns of terrorism. Radicalization can take place in prisons, refugee camps, secular and religious schools, and diasporas as well as online. Part II explores these pathways to terrorism in six chapters.

Chapter 7, titled “At the Crossroads: Rethinking the Role of Education in Preventing and Countering Violent Extremism,” by Thomas K. Samuel (Consultant with UNODC and UNDP) first describes how and why schools and universities have become targets of terrorist recruitment. Then the author explores how and why even socially privileged students can be radicalised and recruited by terrorist organizations. Based on his research in South-East Asia, he advocates that values and qualities such as critical thinking, empathy, and religious and cultural literacy be integrated into subjects taught in schools as well as made part of extra-curricular activities in order to make young people more resilient against extremist ideologies.

Chapter 8, titled “Prevention of Radicalization to Terrorism in Prisons: A Practical Guide,” by Gary Hill (Director, Staff Training and Development of the International Corrections and Prisons Association) draws on his decades-long experience working with correctional institutions, to familiarize the readers with the early signs of radicalization among prison inmates. Prisons have traditionally been depicted as schools for criminals and are now being widely seen as hotbeds for recruitment efforts by extremists. The author reviews prison programs dealing with radicals and presents his concept of “dynamic security” as a way to manage and control the situation.

Chapter 9, titled “Prevention of Radicalization to Terrorism in Refugee Camps and Asylum Centers,” is authored by Barbara H. Sude (former Senior Political Scientist at RAND). She draws on her earlier work in this field and identifies what contributed to the rise of violent militant groups and radicals among refugees confined to camps during major historical migration crises. Then the author turns to the current situation in Africa and Asia where many young people (many of whom have seen nothing of the world outside their refugee camp) can be tempted to join a terrorist group. The experience of Palestinian refugees is one that is not unique in the contemporary world. There are now more than 70 million people who are internally displaced or have become external refugees. In many cases, their situation in camps is comparable to the one of prisoners and radicalization is a clear and present danger if government policies are not responsive to the plight of those driven from their homes.

Chapter 10, titled “Preventing Terrorism from Students of Extremist Madrasahs: An Overview of Pakistan’s Efforts,” by Asad Ullah Khan and Ifrah Waqar (Research Fellows, Institute of Strategic Studies (IISS), Islamabad, Pakistan) explores the situation in religious schools (madrasas) in Pakistan. These serve mainly poor young males who are offered free boarding and lodging while receiving an often fundamentalist religious education. The authors explore the social setting of madrasas and their role in education, politics and terrorism as well as government efforts to reform them, both in terms of broadening the curriculum, and in preventing them from becoming instruments of political entrepreneurs. The authors note that these efforts have so far largely failed due to lack of political will to implement reforms.

Chapter 11 deals with the “Prevention of Radicalization in Western Muslim Diasporas” and has been written by Nina Käsehage (Senior Lecturer at the University of Rostock, Germany). She looks at the situation of Muslims in five countries - Germany, Great Britain, France, Belgium and Denmark - which have all produced homegrown Muslim terrorists who have become foreign fighters in Syria. The author follows the national and international discussions about the causes of radicalization, e.g. the French debate between those who see a ‘radicalization of Islam’ and others who see an ‘Islamization of radicalism.’ The author discusses promising ways of preventing and countering radicalization, such as the Danish
Aarhus model - elements of which have also been introduced in other European countries. The chapter concludes with a set of recommendations, partly based on the author’s own fieldwork in Salafist milieus in several European countries.

Chapter 12 is titled “Prevention of Radicalization on Social Media and the Internet” and is authored by Sara Zeiger and Joseph Gyte (Hedayah International Center of Excellence for Countering Violent Extremism, Abu Dhabi, UAE). They review in detail the methods terrorists employ to spread their propaganda and how they recruit online. The authors also present the theoretical foundations of methods to prevent radicalization on social media and the internet. Subsequently, their chapter explores current and newly emerging prevention and preparedness strategies which address the online space, introducing specific examples, predominantly from Europe, Southeast Asia and East Africa, and showing what selected governments are doing to tackle the problem of online radicalization.

**PART III: Prevention of Preparatory Acts**

Like other purposeful human activities, acts and campaigns of terrorism require preparation. Interference with such preparations (e.g. with arms acquisition or financing) can prevent or foil terrorist attacks. This is the focus of Part III.

Chapter 13, titled “Prevention of Recruitment to Terrorism” has been written by Ahmet S. Yayla (former Chief of Counter-terrorism in Sanliurfa, Turkey and currently Research Fellow at George Washington University, US). The author argues that preventing terrorist recruitment is one of the most effective methods of countering terrorism. Although the recruitment strategies of different organizations may vary, they follow a similar pattern, with recruiters first trying to identify qualified candidates, then build rapport, followed by indoctrination, and finally luring the vulnerable candidates into the clandestine organization. He documents this with examples from his own decades-long experience in Eastern Turkey where he set up a successful program for interrupting and preventing terrorist recruitment after having identified relevant societal factors and triggers that recruiters use to spot and subsequently control the young men and women they recruited.

Chapter 14 is on the “Prevention of Terrorist Financing” by Jessica Davis (former analyst with the Canadian Security Intelligence Service, currently president of Insight Threat Intelligence). The author explores how terrorists raise, use, move, store, manage, and obscure their funds. In doing so, she distinguishes how terrorist cells and individual actors finance their plots and attacks and how terrorist organizations finance their activities. She describes national and international instruments and mechanisms to prevent terrorist financing, and how (and to what extent) bodies like the Financial Action Task Force are able to detect and prevent such activities.

Chapter 15 by Sajjan M. Gohel (International Security Director for the Asia-Pacific Foundation) is entitled, “Prevention of Cross-Border Movements of Terrorists: Operational, Political, Institutional and Strategic Challenges for National and Regional Border Controls.” The author explores how borders are both points of vulnerability for states and opportunities to catch terrorists trying to cross them and how international cooperation is crucial to succeed in intercepting terrorists. The author looks at a number of crucial borders such as those between India, Pakistan and Afghanistan; and those between Turkey and Greece. He analyzes and evaluates obstacles to border security of a political, institutional, and operational/technical nature, specifically focusing on assessing the employed externalisation strategy of the European Union.

Chapter 16 is titled “Prevention of the Procurement of Arms and Explosives by Terrorist Groups” and is authored by Mahmut Cengiz (Professor at the Schar School of Policy and Government, George Mason University, USA). He analyzes how to prevent terrorist organizations from getting a hold of firearms and explosive materials. He discusses several
jihadist and other groups and shows how they procured arms and bomb-making materials. The chapter discusses policy implications and actions that need to be taken in order to prevent terrorist organizations from obtaining weapons. In addition, the chapter explores the challenges that need to be overcome in order to develop a policy model that can be applied to whole regions where terrorist groups operate.

Chapter 17 is titled “Prevention of CBRN Materials and Substances getting into Terrorist Hands” and is authored by Ioannis Galatas (Ret. Brigadier-General and clinical allergy and immunology specialist, Greece). The author explores how terrorists seek to obtain chemical, biological, radiological and nuclear (CBRN) substances. He urges that the CBRN threat should be studied more seriously and that investigators should follow the ways terrorists are plotting their attacks. EU countermeasures and international regulation and control bodies along with preventive measures are addressed. The author identifies existing gaps, thereby facilitating possible solutions and the development of countermeasures that can lead to a better control of CBRN agents and a more efficient management of the risks.

Chapter 18 is titled “Prevention of (Ab-)Use of Mass Media by Terrorists (and vice versa)” and is authored by Alex P. Schmid (Research Fellow, ICCT, The Hague). It explores both the uses of mass media by terrorists and the use of terrorism-generated news by mass media. Ever since the effectiveness of ‘propaganda by the deed’ was discovered in the second half of the 19th century, terrorists have exploited the mass media’s propensity to cover bad news extensively, first with the help of the printing press, followed by radio and television. He analyzes how the media create exaggerated anxiety in the public by sensationalising terrorist-related news. Existing media guidelines for covering terrorist news are discussed and evaluated with an eye on harm prevention resulting from saturation coverage of terrorist incidents.

Chapter 19, titled “Prevention of (Ab-)Use of the Internet for Terrorist Plotting and Related Purposes” is written by Branislav Todorovic (Institute for National and International Security, Serbia) and Darko Trifunovic (Senior Research Fellow Faculty of Security Studies, University of Belgrade). The authors focus on the use of the internet as a tool for assisting terrorist activities and seeks to provide guidance for addressing abuse with the help of legal measures, as well as information and communications technology (ICT) methods. They detail the many possibilities for misuse of publicly available information on the internet for planning, organizing, and executing acts of terrorism and suggest workable measures to counter terrorist plots. They also explore tools for overcoming the anonymity of the internet and describe some of the current legal restrictions and technological shortcomings. The various forms of use/abuse of the internet by terrorists are classified and structured by type and purpose, while possibilities for prevention are discussed for each cluster.

**Part IV: Prevention of, and Preparedness for, Terrorist Attacks**

In Part IV, the focus is on the interface between prevention and preparedness. Ten chapters explore what can, and what has been done, ranging from early warnings to the prevention of cyber-terrorism.

Chapter 20, “The Role of Intelligence in the Prevention of Terrorism (Early Warning – Early Response)” is authored by Ken Duncan (former Chairman of the Interagency Intelligence Committee on Terrorism in the US government). This chapter outlines how intelligence has adapted to terrorism’s ever-changing threat. The author outlines the critical role warning has played and will continue to play in countering and mitigating the terrorist threat. To understand the capabilities and limitations of warnings, the author also examines the factors behind its collection, analysis, production, dissemination, and reception - highlighting the critical relationships between intelligence and law enforcement agencies and between those agencies and their consumers. In addition, his chapter also traces its evolution as part of the US
government’s organizational and operational response to terrorism from the late 1960s until the present, examining both its strengths and weaknesses.

Chapter 21, “Prevention of Low-tech, Lone Actor Terrorist Attacks: The Case of the United States, 1970–2019,” is authored by Joshua Sinai (Professor of Practice in Counterterrorism Studies, Capitol Technology University, in Laurel, Maryland). The author examines the nature of the threat posed by ideologically extremist homegrown lone actors in the United States, based on his analysis of incidents from the period 1970-2019 (listed in an appendix). The research objective is to formulate best practice-based measures to counter lone actor attacks during the formative pre-incident phase. The author examines how some of the plots were discovered and how incidents were resolved, and what measures were or were not applied, particularly in preventing those that had failed. This chapter also discusses what security technologies are being deployed to detect and counter such perpetrators.

Chapter 22, “Prevention of Gun-, Knife-, Bomb- and Arson-based Killings by Single Terrorists” by Annelies Pauwels (Research Fellow at the Flemish Peace Institute in Brussels, Belgium) also focuses on lone actor terrorism and its prevention, doing so by studying lone actor attacks in Western Europe over a period of twenty years. Her main attention is on how to deny potential terrorists the access to weapons and explosives in order to reduce the mortality of attacks. She offers four case studies on each attack type and presents at the end recommendations aimed at further restraining access to weapons and limiting online and hands-on training in the use or manufacturing of arms. The author argues that while a hundred percent safety from lone-actor attacks is probably unattainable, it is possible to diminish their ability to successfully carry out an attack.

Chapter 23, “Prevention of Bomb Attacks by Terrorists in Urban Settings (with a Focus on Improvised Explosive Devices)” is written by Rachel Monaghan (Professor of Peace and Conflict at the Centre for Trust, Peace and Social Relations at Coventry University) and David McLlhatton (Professor of Protective Security and Resilience, Coventry University). The authors note that while much of the literature on the subject has been in direct response to the impact of specific terrorist attacks that have occurred in recent times in many cities, less attention has been devoted to the understanding how policy- and practice-based approaches in disciplines that are not considered mainstream in the counterterrorism discourse can be used to enhance the protection of crowded places. This chapter analyzes, on the one hand, the question, “what measures have been undertaken?” and on the other hand, but to a lesser extent, “who should be responsible for counterterrorism-related protective security measures?”

Chapter 24, “Prevention of Kidnappings and Hostage-Takings by Terrorists”, is authored by Alex P. Schmid, the editor of this Handbook. This chapter looks into what can be done to prevent kidnappings and acts of hostage taking, focusing, on the one hand, on the seizure phase and, on the other hand, on the negotiation phase where the prevention of loss of lives among the hostages becomes paramount. Criminal and political acts of kidnapping and hostage-taking, local and transnational abductions and barricade and non-barricade types have their own dynamics and are therefore not always comparable. Successful kidnappings where governments pay large ransoms can encourage imitations and become contagious, thereby trading short-term prevention of loss of lives for higher risks of future abductions.

Chapter 25 by Susanne Martin (Political Science Department, University of Nevada, Reno) addresses the difficult subject of “Preventing Suicide Attacks by Terrorists” with a special focus on Israel which experienced two Palestinian intifadas marked by “martyrdom” operations. She finds that while counterterrorism efforts in Israel and those involving the hijacking of passenger planes have been fairly successful, until now no remedies for the sources of the violence that inspire groups to use suicide attacks or individuals to sacrifice their lives and those of their victims have been found. However, tactical solutions can and do reduce the frequency and severity of suicide attacks.
Chapter 26, “The Terrorist Threat to Transportation Targets and Preventive Measures” has been written by Brian M. Jenkins (Director of the National Transportation Security Center at the Mineta Transportation Institute in California). The author addresses both aerial hijackings and terrestrial attacks on commuter trains and busses, drawing from a unique database of national and international incidents. He notes that the relatively successful model developed to counter aerial hijackings cannot be replicated on the ground due to the high volume of local commuters. Instead of establishing security checkpoints, terrestrial transportation operators ought to seek to mitigate casualties through environmental design and rapid intervention, while also enlisting passengers themselves in detecting suspicious behavior.

Chapter 27, titled “Layers of Preventive Measures for Soft Target Protection against Terrorist Attacks” by Alex P. Schmid (Research Fellow, ICCT) analyses the shifting focus of terrorist targeting and discusses the many audiences terrorists seek to influence by attacking specific victim groups. He presents mainly mid- and down-stream counter-measures and develops a security concept including 13 Layered Preventive Measures (LPM) for reducing the risk of attacks on soft targets. In the concluding section, the author juxtaposes his own LPMs with the Good Practices (GP) recommended in 2017 by the Global Counter Terrorism Forum which consists of an equal number of measures. As an Appendix, the chapter lists ‘12 Rules for Preventing and Countering Terrorism’, a guideline which the author originally developed when he was Officer-in-Charge of the Terrorism Prevention Branch of UNODC.

Chapter 28, “Prevention of Terrorist Attacks on Critical Infrastructure” is authored by Anneli Botha (Senior Researcher at the Department of Political Studies and Governance, University of the Free State in South Africa). She notes that such attacks have been on the increase but finds that while the threat of cyber-attacks against critical infrastructure is a reality, the use of firearms and explosives still remains the preferred modus operandi. However, the author also notes a growth of drone attacks. She argues that developing preventative measures must start with understanding the “enemy” - the motivations and capabilities of terrorist organizations. To get ahead of the curve, it is necessary to make continuous risk-, threat- and vulnerability- assessments and implement measures for anticipating infrastructure attacks.

Chapter 29, “Cyber Attacks by Terrorists and Other Malevolent Actors: Prevention and Preparedness. With Three Case Studies on Estonia, Singapore and the United States” has been written by Shashi Jayakumar (Executive Coordinator, Future Issues and Technology at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore). The author examines attacks against computer infrastructure and Critical Information Infrastructure (CII) by all actors with relevant capabilities - not just non-state groups such as Al-Qaeda or ISIS. He notes that while conventional terrorist groups might have the intention to launch major cyberattacks, they do not yet have the resources and skills to carry out the type of attacks that might lead to major loss of life. His wide-ranging chapter also focuses on technical aspects of cyber protection, system resilience, risk mitigation, as well as nurturing human talents within a viable cyber ecosystem.

Part V: Preparedness and Consequence Management

Here the focus of five chapters is on what to do to minimize harm should prevention fail, and how this can be done, exploring victim- and human rights issues among others.

Chapter 30 on the “Prevention of Lasting Traumatization in Direct and Indirect Victims of Terrorism” is authored by Shannon Nash (Network Manager of the North American and Arctic Defence and Security Network). In her chapter, the author reviews findings of important studies on how to reduce risk factors contributing to lasting traumatization of terrorism victims. The chapter identifies a variety of responses and mental health strategies to mitigate damage, including support for first responders, and the promotion of resilience in children. She also
focuses on disaster planning, stressing that preparations occurring both before and after an attack can contribute toward more effective responses, based on a public health model.

Chapter 31 focuses on the “Prevention of Public Panic in the Wake of Terrorist Incidents” and is jointly co-authored by Juan Merizalde, John D. Colautti, and James J.F. Forest (all associated with the Center for Terrorism & Security Studies, University of Massachusetts, Lowell). The authors note that studies on community resilience indicate that being well prepared, effectively communicating accurate and relevant information and empowering citizens to take recommended actions, all help to significantly reduce fear and anxiety in times of crises. While one of the objectives of terrorists is to create public panic, studies show that such an outcome is unlikely; studies of public behavior following terrorist incidents conclude that most people are logically-reacting, rational beings who tend not to panic or be frozen in fear. Following a review of research findings, the chapter concludes with a brief discussion of policy implications.

Chapter 32 is titled “Prevention of Major Economic Disruptions Following Acts of Terrorism – The Case of the Bali Bombings of 2002 and 2005” and is authored by Richard J. Chasdi (Department of Political Science, George Washington University). The writer focuses on the economic consequences of terrorism, with particular attention to the tourism industry and related services sectors. By selecting a twice hit location (Bali, Indonesia) with a three years interval between the terrorist attacks, lessons learned and not learned emerge. The author applies a three-level analysis to the consequences, looking at international, national and local responses, which can also serve as a framework for similar studies in the future.

Chapter 33, “Prevention of Revenge Acts and Vigilantism in Response to Acts and Campaigns of Terrorism” by Marie Robin (Researcher at the Centre Thucydide at Université Paris 2 Panthéon-Assas) explores an important, but under-researched, aspect of terrorism -the desire for individual revenge. This desire becomes especially strong when government responses are considered weak or inadequate by sectors of society. Since terrorism is often a strategy of provocation, giving in to this understandable, but ultimately counter-productive impulse needs to be countered. The author examines the dangers posed by vigilantism and concludes with offering recommendations on how to deal with private revenge acts and vigilante efforts to restore “order” outside the rule of law.

Chapter 34 looks at the “Prevention of Human Rights Violations and Violations of International Humanitarian Law while Fighting Terrorism” and is authored by Tom Parker (former UK Intelligence Officer and subsequently UN Consultant). The author examines the role of human rights violations by state actors in fuelling non-state terrorism. Based on rich historical and contemporary materials, he shows how, again and again, governments fall into what he terms “the terrorist trap,” giving in to provocations rather than devising a strategy not dictated by the terrorists. He argues that adhering to higher moral standards than terrorists is crucial in winning the battle for the hearts and mind of the people. Adhering to international human rights law does not hinder but helps prevent states from falling into the terrorists’ trap.

Chapter 35, the volume’s concluding chapter 35 "Terrorism Prevention – The UN Plan of Action (2015) and Beyond" is from the hands of the editor, Alex P. Schmid. He compares findings and recommendations of the contributors of this Handbook with the Plan of Action to Prevent Violent Extremism presented by the UN Secretary-General in late 2015 and finds that there are many similarities. He then compares these with findings based on the science of System Analysis and looks at statistical correlations of terrorism and also notes a good fit. In other words, the main preventive measures presented in this volume and in the UN Plan of Action are based on solid empirical foundations. Their ultimate success stands and falls with national and regional implementation plans. Finally, the author sketches elements of a generic terrorism prevention strategy and concludes with four big prevention ‘Lessons Learned’.

An extensive General Bibliography on the prevention of radicalization, extremism and terrorism as well as preparedness has been compiled by Ishaansh Singh (Terrorism Research
Initiative). It can be found at the end of the volume. However, each chapter also has its own bibliography while also offering a list of clickable, web-based resources.

Each chapter of the *Handbook* is self-contained and can be read on its own as there are few cross-references. Information about the contributors to this volume can be found at the end of each chapter.

Despite its size, the *Handbook* has its limitations. Except for a few chapters (Chapters 4, 6 and 34), this volume does not address the issue how to prevent - and prepare for - state or regime terrorism. While the editor has dealt with state terrorism and repression in some of his previous work, he decided not to focus on this problem in the present *Handbook* due to space limitations.
Endnotes


3 Crawford Neta C., and Catherine Lutz, ‘Human Cost of Post-9/11 Wars: Direct War Deaths in Major War Zones, Afghanistan and Pakistan (October 2001 – October 2019); Iraq (March 2003 – October 2019); Syria (September 2014-October 2019); Yemen (October 2002-October 2019); and Other,’ Costs of War Project, Brown University, Providence, RI, 13 November 2019. Available at: https://watson.brown.edu/costsofwar/files/cow/imce/papers/2019/Direct%20War%20Deaths%20COW%20Estimate%20November%2013%202019%20F.


Chapter 2

Terrorism Prevention: Conceptual Issues (Definitions, Typologies and Theories)

Alex P. Schmid

This chapter serves to outline a framework for the analysis of terrorism. Key concepts (prevention, terrorism, extremism, radicalization) are defined and discussed, as are prevention of radicalization and prevention of extremism as alternative frameworks related to terrorism prevention. The difficulty of theory formation is outlined and some promising borrowings from crime prevention theory are introduced. Typologies of terrorism and prevention are presented and a tri-partition into upstream-, midstream- and downstream-terrorism prevention is suggested, illustrated by examples of measures to be taken, or intervention to be made, for each of these phases. In addition to suggesting working definitions for terrorism prevention and preparedness, the chapter also features a short appendix with definitions of prevention in the fields of conflict, crime, and violence.

Keywords: definition, extremism, prevention, preparedness, radicalization, terrorism, theory, typology.
Given the fact that so much has been written about terrorism since 9/11, one cannot help wonder why a major handbook like this one has not been published a long time ago. After all, nobody contests Benjamin Franklin’s dictum that “an ounce of prevention is worth a pound of cure” (he was talking about medicine, but the idea has been applied to many other fields). Why then did it take such a long time for a comprehensive volume like this one to see the light of day? There are many possible answers. For example, the effectiveness of prevention is difficult to measure in the short term and spending effort and money on something that has not yet occurred and might not happen at all is difficult, given more urgent (though not necessarily more important) demands on scarce resources. This also applies to research on terrorism prevention. While much is written on the subject (see bibliography at the end of this Handbook), it more often than not lacks depth and empirical grounding.

In terms of social science, one problem is that there is no general theory of prevention, since that would necessitate a predictive theory of the future. Rik Peeters has rightly observed, that “prevention takes a not (yet) existing reality as the basis for intervention in the present.” He further noted that:

“prevention implies….a belief in a certain ability to anticipate the future and in a certain ability to choose among alternative courses of action in order to avert this future. It depends on the construction of a causal scheme between future events and actions taken to avoid them. Consequently, prevention implies the potential of backward reasoning to avert a certain imaginable future.”

Such anticipatory reasoning comes more often than not in the form of more or less educated guesses rather than being based on more formal techniques such as scenario-constructions (i.e., best case, worst case and most likely case) depending on the strengths and directions of key drivers. Is there a theory of prevention?

Prevention: In Search of Theory

Under the heading “Theories of Prevention,” Ian Gough from the London School of Economics noted in 2013 that such theories “are notable for their absence.” Prevention - independent from the subject area on which it is focused - is a challenging concept. How can one establish a causal relationship between the impact of a set of cautionary interventions or preventive measures and an outcome that is a non-event, namely, in our case, the absence of acts of terrorism? After all, the same non-event outcome might possibly have come about anyway, without active interventions aiming at the removal or mitigation of causes and without targeting presumed drivers of radicalization, extremism and terrorism?

While we are all interested in the future since we are, as someone dryly observed, going to spend the rest of our lives there, we only have very limited control over our future. Yet we can control (although never fully) at least some parts of the future, namely those parts we are willing and able to actively shape ourselves, rather than leave that future to the vagaries of free markets, the electoral opportunism of political leaders who dismiss science, or to the phantasies of demagogues and preachers who pretend that their ideology or religion has all the answers.

Rik Peeters also cautioned that “the way you look at the world determines what you see and the action you are likely to take.” In the absence of a realistic understanding of the drivers of change in our societies we might, if we are not careful, be barking up the wrong tree. The best way to approach the subject is by using the instruments of science that allow us to methodologically question our assumptions and develop theories that can be tested. That is easier said than done in the field of prevention. Ian Gough has pointed out that “Prevention policy is built on two basic foundations, both of which are contested concepts. First, scientific
understanding of cause and effect and the possibility of prediction... Second, prevention policy presumes some capacity for controlled intervention by government in social life.”

In the field of terrorism prevention, there are many more questions than answers. Here are but a few of the questions that deserve closer scrutiny and adequate answers:

- What exactly do we mean by “terrorism prevention”?
- What are the principal causes and drivers of terrorism that need to be addressed and, to the extent possible, neutralized or turned around to achieve effective prevention?
- What sort of measures and interventions are most appropriate for up-, mid- and down-stream terrorism prevention?
- How can one prevent terrorist attacks plotted in one country, executed in a second country against a target belonging to a third country?
- How can one prevent more or less spontaneous single actor attacks against random civilians in public spaces, performed with weapons as common as knives and cars?
- Should we be searching primarily for preventive, tactical operational measures, or aim for structural strategies of prevention?
- Should we be concentrating on reducing the capabilities of terrorists, or diminishing their motivations?
- Should we prioritize the strengthening of the resilience and preparedness of their potential victims and targets?
- Should we prepare for high-impact (but low probability) attacks (e.g. CBRN) or focus mainly on high probability (but low-impact) attacks (e.g. by knife)?
- How should we assess, monitor and evaluate prevention and preparedness efforts?

In this chapter, the main focus is on the first of these questions, “what exactly do we mean by terrorism prevention”? It has been said that a problem well-defined is a problem half-solved. While this is certainly an exaggeration, there is more than a grain of truth in it: conceptual issues need to be taken seriously. Building theories on shaky conceptual foundations is like building on sand.

What then is terrorism prevention? Answers have been sought and given by scholars and government agencies. Here, for instance, is a recent authoritative joint description of the concept of “terrorism prevention” by three key stakeholders in the US government. It represents the joint wisdom of the National Counter Terrorism Center (NCTC), the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) under the Trump administration:

What is Terrorism Prevention? Terrorism Prevention, previously known as Countering Violent Extremism (CVE), is a multi-agency, multi-disciplinary, proactive approach against the many forms of terrorism ideology. Terrorism Prevention works to protect our nation from terrorist threats, and remains our highest priority. It utilizes prevention, intervention, and disengagement efforts. The principles and strategies used in Terrorism Prevention are similar to those applied in community policing, counter-drug, and counter-gang initiatives. (...) Violence reduction is a proactive approach to counter efforts by terrorists, and address the conditions that allow for violent extremism. ...The ability to recognize and address possible terrorist activity is critical in the prevention of terrorist attacks.
This official American government definition – if you can call this listing a definition – equates it first with “countering violent extremism” (CVE), a similar concept that was quietly shelved in January 2017 when Donald Trump became the 45th president of the US. We can further learn from this definition that the principles and strategies are similar to those applied in counter-drug initiatives. Given the lack of success in nearly fifty years of the American War on Drugs declared by President Nixon in June 1971, this does not bode particularly well.

DHS - one of the three US agencies behind this definition - clarified the issue somewhat in a different document by identifying four lines of activities in terrorism prevention:

- promoting education and community awareness;
- countering terrorist recruitment and propaganda;
- providing early warning of individuals who have radicalized; and responding to cases of radicalization to violence;
- keeping suspects and individuals convicted of terrorism-related offenses from returning to violence.

The emphasis of terrorism prevention here is on ‘soft power’ - tools that reduce the need for more lethal counterterrorism efforts, focusing on activities on individual and community levels. In another publication, dating from 2015, DHS referred, when discussing prevention, to its own “risk-based, layered approach” which utilizes new technologies to “detect explosives and other weapons, help protect critical infrastructure and cyber networks from attack [and] build information-sharing partnerships.” This points more in the direction of preparedness, the second theme of this volume.

After this first look at one government’s definitions, let us turn briefly to a more academic definition of terrorism prevention, one suggested by Peter Romaniuk (currently Executive Director of The Soufan Center) and Naureen Chowdhury Fink (an academic who joined the UK mission to the UN Security Council). They see – or saw, back in 2012 – terrorism prevention as a derivative of the concept of countering radicalization and defined it as “measures designed to counter the ideas, narrative, or message advanced by extremists and complement operational preventive efforts.” Terrorism prevention, Romaniuk and Fink added, aims to “prevent non-radicalized populations from becoming radicalized. The objective is to create individual and communal resilience against cognitive and/or violent radicalization through a variety of non-coercive means.”

To portray terrorism prevention as prevention of radicalization is one viable approach. However, this is arguably also too narrow a framework since it implies that only radicals commit acts of terrorism. Yet, there is considerable evidence of, for instance, reactionary (counter-) terrorism by opponents linked to the state and of false flag operations executed by agents of rogue regimes; they are decidedly not radicals or radicalized although what they do is “extreme” compared to “normal” politics. The link between radicalism and radicalization, and even more so, between radicalism and terrorism, is not always present or direct.

In addition, radicalism should also not be confused with extremism. More recently, some equate terrorism prevention with the prevention of “violent extremism.” Extremism, like radicalization, can and does indeed precede many manifestations of terrorism. Yet prevention of terrorism, prevention of radicalization and prevention of extremism, are, as we shall see in this chapter, not quite the same - although there can, at times, be substantial overlap.

While the problem of terrorism prevention is partly linked to the difficulties related to prevention in general, it also rests on the fact that we have many definitions of “terrorism” which are remarkably different from each other. While the UN has been debating the definition issue – with interruptions - since 1972, no consensus has yet emerged among the 193 members of the UN General Assembly (UNGA) regarding terrorism. We have a few regional definitions of terrorism (e.g., by the European Union or by the African Union) and many more national
definitions (with some governments having more than one), yet we still lack a universal legal definition of terrorism that has the full authority of the UNGA behind it.

Does this matter? Why is it important? The definition problem is also a response problem – the broader a definition, the more terrorism there is that ought to be countered and the more difficult it becomes to prevent it.\textsuperscript{17} If countries have different definitions of terrorism, extradition of terrorist suspects and mutual legal assistance become more difficult and often impossible – a phenomenon sometimes expressed with the misleading phrase “one man’s terrorist is the other man’s freedom fighter.”

Definitions are important and part of the lack of success in preventing terrorism has to do with a lack of rigor on the conceptual side. As J.M. Berger, an American researcher, has put it:

“Many factors contribute to the stagnation and inefficacy of the field known as Countering Violent Extremism (CVE) or Preventing Violent Extremism (PVE). Among the most important problems are a lack of definitions for key terms, a lack of consensus models for extremism and radicalization, and a lack of interest in understanding extremism as a cross-ideological phenomenon.”\textsuperscript{18}

Let us therefore take a closer look at three key concepts linked in this volume to prevention: terrorism, extremism, and radicalization.\textsuperscript{19}

\textbf{Terrorism}

Our object of prevention – terrorism – is a multifaceted phenomenon. Monty Marshall and Ted Gurr, writing in 2005, noted:

“Terrorism, as a political act, stands at once at the nexus between individual and collective action, the emotional and the rational, the conventional and the unconventional. It can be the strongest form of protest, the weakest form of rebellion, or a specialized tactic in a broader process of tyranny or warfare.”\textsuperscript{20}

There are many types of terrorism, the most prominent ones being:

- single-issue terrorism;
- lone wolf/actor terrorism
- vigilante terrorism;
- separatist (ethno-nationalist) terrorism;
- left-wing terrorism;
- right-wing terrorism;
- religious terrorism;
- cyber-terrorism;
- chemical, Biological, Radiological and Nuclear (CBRN) terrorism;
- state (or regime) terrorism.\textsuperscript{21}

Should/can terrorism prevention address all of the manifestations above? Or should it go even beyond these ten types of terrorism and also address political violence in general since some governments use terrorism and political violence more or less as synonyms? While terrorism is, in most (but not all) cases, a form of political violence, there is, however, a great deal of political violence and irregular armed conflict activity that is not terroristic - some of it worse, some of it less bad.\textsuperscript{22} If terrorism prevention should cover all the manifestations from
the entire spectrum of political violence as well, including some forms of armed conflict not regulated by international humanitarian law, prevention would become an endless and indeed almost impossible task.

Terrorism not only comes in many variants, as the list above makes clear, terrorism itself has also been defined in many ways. In the *Routledge Handbook of Terrorism Research* (2011), Joseph Easson and Alex Schmid listed no fewer than 260 different academic, national and regional definitions. However, we still do not, as noted above, have a legally binding definition of terrorism as an international crime, one agreed upon by the UNGA – despite the fact that an Ad Hoc Committee on Terrorism and a Working Group, established by the Sixth (legal) Committee of the General Assembly of the UN, has been looking for more than twenty years for a single definition all 193 UN member states can agree on. All it produced so far is this draft definition which is both broad and vague:

**Art. 2.1. of draft UNGA Comprehensive Convention on International Terrorism**

“Any person commits an offence within the meaning of the present Convention if that person, by any means, unlawfully and intentionally, causes:

a) Death or serious bodily injury to any person; or
b) Serious damage to public or private property, including a place of public use, a facility or to the environment; or
c) Damage to property, places, facilities or systems referred to in paragraph (b) of the present article, resulting or likely to result in major economic loss, when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.”

The accumulation of “anys” - any person, any means, any act - in this draft definition indicates a lack of precision which can have serious implications when it comes to terrorism prevention. While the UNGA has been unable to reach a consensus definition due, inter alia, to conflicting views on issues like the inclusion or exclusion of “people’s struggle for self-determination” (especially regarding Palestine and Kashmir), an academic definition of terrorism that is not legal but social-scientific in nature has gained a certain measure of acceptance among scholars. Based on three rounds of consultations with some 200 experts and professionals, the following formulation emerged in 2011:

“Terrorism refers, on the one hand, to a *doctrine* about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence and, on the other hand, to a conspiratorial *practice* of calculated, demonstrative, direct violent action without legal or moral restraints, targeting mainly civilians and non-combatants, performed for its propagandistic and psychological effects on various audiences and conflict parties. Terrorism as a tactic is employed in three main contexts:

1. illegal state repression;
2. propagandistic agitation by non-state actors in times of peace or outside zones of conflict, and
3. as an illicit tactic of irregular warfare employed by state- and non-state actors.”
The doctrine referred to in this academic consensus definition was developed in the second half of the 19th century when the inventions of dynamite and the rotary press began to interact. At that time, terrorism – a term originating from the French revolution in 1793-94 and applied first to crimes of state - was called “propaganda of [or:by] the deed” and referred mainly to the revolutionary agitation of anarchists and socialists in Russia, France and some other European countries. Since the 1870s, the upcoming rotary press allowed terrorists to reach the masses through commercial and political party-owned newspapers. Gone were the days when, after an assassination attempt on an oppressive ruler, the terrorists had to place posters on city walls to explain to the people why they did what they did. The newspapers, eager to sensationalize such deeds, would from then on do the job of spreading the news that was terrible to some (the victims and those who identified with them) but not to others (those who shared some of the same goals as those motivating the terrorists) depending on which side of the proverbial political fence they were sitting.

After the 19th century rotary press came, in the 20th century, radio. It became mainly an instrument of state terrorism, as were the news reels shown in cinemas before the main movie in the years between the two world wars and beyond. Later, from the 1950s onwards, television would do the job of spreading propaganda on behalf of non-state terrorists. Today, with the internet, we have, according to Steven Pinker, reached a stage where terrorism has simply become a “by-product of the enormous reach of mass media.” While the situation is not as “simple,” there is considerable truth in this statement. In the 1980s, British Prime Minister Margaret Thatcher had already observed that publicity is the oxygen of terrorism. Today’s mass as well as the social media propagated on the internet give contemporary terrorism much of its over-sized punch.

Mass media and social media are major structural factors that facilitate terrorism. They give terrorists attention, spread their grievances and demands and allow them to get respect and, in a few cases, even legitimacy among some of those who share their grievances or their goals, if not necessarily their methods. The core of terrorism is the combination of violence and communication adding up to armed propaganda. The diagram below, depicting the triangle of terrorism, explains the indirect strategy of terrorism - the immediate victim is not the main or ultimate target. Rather, the use of violence against certain individuals and groups of people serves the purpose of agitation, intimidation or coercion, being the message generator to reach an audience much larger than the direct victims and the local witnesses present at the crime scene.

**Figure 1. The Triangle of Terrorism**
From the point of view of the history of ideas, terrorism is first of all “propaganda by the deed” - a performative communication strategy for psychological manipulation whereby mainly unarmed civilians - who are often complete strangers to the perpetrators of violence - are deliberately victimized in order to impress third parties (e.g. intimidate, coerce or otherwise influence a government or a section of society, or public opinion in general), with the help of portrayals of demonstrative violence in front of witnessing audiences and/or by means of induced coverage in mass and social media.\(^\text{31}\)

If one could eliminate, or at least greatly reduce, the communicational spread of the terrorists’ demonstrative public performances of acts of violence for purposes of publicity, terrorism would lose most of its appeal and attraction. However, breaking the communication link between terrorist victims and target audiences\(^\text{32}\) would imply some form of censorship which is a very high price to be paid for what in most societies is still more of a nuisance rather than an existential threat. Nevertheless, attempts to block — or at least reduce — terrorist access to mass audiences are on the rise and constitute one of the methods of prevention and control of terrorism, used increasingly by non-democratic regimes. The arrival of the internet which now reaches, and links more than half of mankind has made the task of controlling harmful effects of instant communications of violence for effect much harder for democratic states, despite the fact that the large social media platforms (e.g., Facebook, Google, Twitter, etc.) now have thousands of so-called “content moderators” charged with removing terrorist and other undesirable content from the internet.\(^\text{33}\) Non-democratic governments (e.g., China) have used more forceful approaches to silence social and other media. Since terrorism is, at its core, violence for communication,\(^\text{34}\) prevention of terrorism cannot exclude interventions trying to minimize if not neutralize the communication strategies of terrorism.

On the basis of this communication function, acts or campaigns of terrorism seek to intimidate and terrorize the public or sections thereof, to discipline, control or dissuade targeted (sub)groups or aim to enforce their obedience. On the other hand, some spectacular terrorist acts can also mobilize sympathizers and turn some of them into supporters and new recruits. Acts of terrorism can serve to win specific political concessions (such as the release of prisoners) from the government but can, at times, also serve to provoke over-reactions from the regime in power in the hope of splitting and polarizing communities.\(^\text{35}\) In short, acts, and especially campaigns of terrorism are instruments of influence warfare between conflict parties that involve not just the government and rebel forces but also sectors of our communities at home and abroad, all linked by the mass and social media as the nerve system of an increasingly global society. This multiplicity of functions and purposes of terrorism makes its prevention difficult and challenging.

A Typology of Prevention

The prevention literature, which has been spearheaded by the public health field, distinguishes between various intervention points to counter unwanted, harmful occurrences. In the 1960s, R.S. Gordon Jr. introduced in the medical sector a tri-partition of prevention levels, based upon the costs and benefits of delivering the intervention (e.g., inoculation during epidemics of disease) to the target population group:

- Universal prevention – aimed at the entire population, involving strengthening public resilience;
- Selective prevention – focusing on the sub-population whose risks of developing problems is already at an elevated, above average, group level, specific vulnerable sectors of society;
• Indicated prevention – involves a screening process, and aims to identify individuals who exhibit early signs of early conduct problems and/or having an increased risk for such problems, but currently not having any.\textsuperscript{36}

This basic tri-partition has sometimes also been labelled primary, secondary and tertiary prevention.\textsuperscript{37} Other names have been: early phase, middle phase, and late phase prevention,\textsuperscript{38} or upstream, midstream, and downstream prevention.\textsuperscript{39} Unfortunately, there is little correspondence in the literature about the exact boundaries between these terms, i.e., where primary prevention ends, and secondary prevention and later tertiary prevention begins, as Ian Gough has pointed out.\textsuperscript{40} The same is true about the phase or the stream prevention models.

This basic tri-partition has also been adopted and adapted in the field of terrorism, radicalization and extremism prevention but, again, there is no consensus where the lines should be drawn between the three stages in the literature on the subject. The Danish Prevention of Extremism Pyramid, for instance, breaks prevention down in three temporal phases:

• Early preventive measures (for everyone): The primary section of the pyramid – the early preventive level – includes initiatives aimed at the whole of society, but focuses predominantly on young people. The purpose of initiatives at this level is to promote well-being, development and active civic citizenship, and to prevent the development of problematic behavior. The goal is to strengthen democratic, critical and social skills, and build resilience among young people without explicitly addressing the challenges of extremism and radicalization.

• Anticipatory measures (for persons vulnerable to radicalization): The secondary “anticipatory” level – the middle part of the pyramid – includes initiatives that target individuals who are already showing signs of concern with regard to radicalization. Measures here largely overlap with crime prevention measures.

• Direct intervention measures (persons in extremist environments): The tertiary level involves direct interventions targeting individuals who are part of an extreme environment and have already committed crimes, or who are at risk of doing so. The purpose here is to prevent (further) crimes and support their disengagement from extremist environments.\textsuperscript{41}

The Danish model includes elements of mid-stream prevention while most other models are limited to tertiary or downstream terrorism prevention. This model focusses on the prevention of extremism, rather than the prevention of terrorism, although it treats these terms as more or less overlapping. While much attention has been given to who should be prevented from being radicalized, less attention has been given to who should do the prevention work. Originally, it was held to be the task of the police or the military. Later, a “whole-of-government” approach became popular, which includes departments which focus on education (since radicalization also occurs among school-going youth), the treasury (since the financing of terrorism has to be stopped), as well as other departments. More recently, a “whole-of-society” approach has been propagated, with terrorism prevention becoming a task of all citizens, beginning in the family (where parents have to notice and report signs of radicalization), and progressing to civil society associations (e.g., sport), public health (e.g., mental health institutions) and social media (to report hate speech and glorification of violence). If we look at who prevents acts of terrorism in concrete cases, it becomes clear that the role of civil society is important. A study by the Norwegian Police Security Service (PST) on how terrorist attacks in 13 countries in Europe, North America, Australia and New Zealand were averted in the period 2012-2019 showed the following distribution:
Figure 2. Terrorist Attacks Prevented in 13 Western Countries, 2012-2019 (n= 91)

By the Intelligence/Security Services: 43%
By the Police: 28%
By the Public: 18%
By Public/Private Institutions: 11%

Tips from family and acquaintances of terrorist plotters were contributing to the uncovering of attacks in 10 percent of the cases. In 45 percent of the cases attacks could be prevented as a result of monitoring the online activity of militants. Tips from third parties were the first indicators in 23 percent of the plots. Police uncovered terrorist plots while investigating (other) criminal activities in 10 percent of the cases.42

From these figures it is clear that prevention is not only the work of intelligence services and the police, but results also from the vigilance of parts of the public.

The choice of framework is important: should we focus on the prevention of terrorist crimes, or the prevention of ideological extremism, or the prevention of radicalization of “vulnerable youth”? In terms of theory formation, the prevention of terrorism as crime is most advanced (being an extremist or becoming radicalized is not a crime per se in most jurisdictions). Let us have a brief look at what criminology has to offer before looking at the prevention of extremism and radicalization.

Borrowing from Crime Prevention Theory

When it comes to terrorism prevention, some of the most inspiring ideas have come from the literature on crime prevention. One of the first attempts can be found in the work of Ronald Clark and Graeme Newman. They tried to transfer some principles from situational crime prevention to terrorism prevention. Key to their approach is to reduce opportunities and rewards for crime by applying five principles:

1. Increase the effort: target hardening (including concealing targets) and controlling tools/weapons;
2. Increase the risks, e.g., by reducing anonymity and strengthening formal surveillance;
3. Reduce provocations: reducing frustrations and stress and discouraging imitation;
4. Reduce the rewards: removing targets, disrupting markets, and denying benefits;
5. Remove excuses: setting rules, alerting conscience and assisting compliance.43

Clark and Newman argue that more attention should go to the reduction of the opportunities for terrorist attacks. This can be done by protecting the most vulnerable targets, controlling the tools and weapons needed by the terrorists, and by removing the conditions in our environment that make terrorist attacks easy to perform. “Red Teaming,” or trying to do what terrorists are likely to do as a training exercise, exposes weaknesses in our defenses and allows security agencies to develop better protection where it is most needed, limit accessibility to likely targets, and anticipate the forces needed to counter a potential attack. The situational approach to terrorism prevention looks closely at terrorists’ modus operandi, expertise, and the tools and weapons available to them.

Clarke and Newman’s approach does not rely on changing the “hearts and minds” of terrorists – the aim of deradicalization – but focuses on exploring how rational terrorists seek to accomplish their tasks. Once that is understood, their opponents have to (i) increase the effort involved; (ii) face the increased risks of failure; (iii) seek a reduction in the rewards of
terrorism; and (iv) have fewer temptations, provocations and excuses to do what they originally wanted to do.44

Based on these (and other) principles, Prof. Tore Bjørgo from the University in Oslo, published a brief, but seminal, study of terrorism prevention in 2013. It is also based on proven crime prevention mechanisms and measures.45 Prof. Bjørgo uses the concept of “prevention” in this context as referring to “...reducing future act of terrorism or other crimes, or reducing the harmful consequences of such acts, by proactive measures.”46 Here are his nine mechanisms for preventing terrorism:

1. *Establishing and maintaining norms* to delegitimize terrorism and the use of violence;
2. *Reduce violent radicalization* and emergence of terrorism;
3. *Deterring involvement in terrorism* by threat of retaliation or punishment;
4. *Pre-emptive disruption* of planned terrorist attacks;
5. *(Incapacitation of (potential) terrorists by removing their capacities for carrying out violent action;*
6. *Protecting vulnerable targets* by increasing difficulties, costs and risks for (potential) terrorists;
7. *Reducing harmful consequences* of terrorist acts;
8. *Reducing rewards* for carrying out terrorist attacks;
9. *Disengagement from terrorism* by making individuals and groups discontinue their involvement in terrorism.47

Bjørgo’s volume *Strategies for Preventing Terrorism* is an excellent starting point to advance our thinking on the subject.48 He introduces not only these nine preventive mechanisms, but also outlines the measures that need to be taken to implement these and explains in his book who has to take them against whom and what the ups- and downsides of each of the proposed measures are.49

However, a narrow crime prevention framework for terrorism prevention, useful as it is, tends to neglect the political or ideological dimension of terrorism – the latter of which is sometimes referred to as “extremism.” It is to this we turn to next.

**Terrorism Prevention as Prevention of Extremism**

Since the international community – meeting in the General Assembly of the UN – could not agree on a definition of terrorism, the term has, in political discourse, often been replaced with the broader and even more vague concept of “violent extremism.” This evades – but does not solve – the definition problem. The concept “violent extremism” originated in UK policy circles around the time of the attacks on the London transport system on 7 July 2005.50 It gained wider currency in US policy making circles where a distinction was introduced between “violent extremism” and “non-violent extremism.”51 The concept of violent extremism served to avoid offending Muslims in the US and Arab regimes allied with the US that did not wish “peaceful Islam” be associated with terrorism.52 In recent years, extremism and its prevention has led to a great deal of research. As of mid-March 2019, no less than 12,013 papers dealing with “preventing violent extremism” could, for instance, be downloaded from a website storing academic papers.53

Since there is a widely held – and often correct – assumption that terrorism is encouraged, if not caused, by extremism, we need to look into this assumption more closely. Again, we face a definition problem. There are several definitions of extremism around - though not nearly as many as for terrorism. The Danish government, for instance, defined extremism in 2016 in this way:
“Extremism refers to persons or groups that commit or seek to legitimise violence or other illegal acts, with reference to societal conditions that they disagree with. The term covers e.g. left-wing extremism, right-wing extremism and Islamist extremism.”

While this is a practical definition, it still falls short of addressing adequately the ideological dimension. What then is “extremism”? Unlike radicalism, which has a long history in politics, extremism has a shorter, but darker history, closely linked to the rise of fascism and communism in the Western world and emerging in reaction to the catastrophe of the First World War with its 20 million deaths (half of them civilians) and its 21 million wounded - a war that had brought about the fall of four empires (Russian, Ottoman, German and Austrian-Hungarian). Among the losers of the First World War, poisonous nationalist revanchism emerged, partly in the form of Fascism. Some of the surviving returning soldiers from the front were more attracted to Communism which came to power in Russia in late 1917. The American political scientist Manus Midlarsky studied the rise of extremist political movements after World War I and offered this definition of political extremism:

“the will to power by a social movement in the service of a political program typically at variance with that supported by existing state authorities, and for which individual liberties are to be curtailed in the name of collective goals, including the mass murder of those who would actually or potentially disagree with that program. Restrictions on individual freedom in the interests of the collectivity and the willingness to kill massively are central to this definition: these elements characterize all of the extremist groups considered here.”

More recently, J.M. Berger came up with an elegant and more concise definition of extremism:

“Extremism refers to the belief [that] an in-group’s success or survival can never be separated from the need for hostile action against an out-group…. Hostile action can range from verbal attacks and diminishment to discriminatory behavior, violence, and even genocide…. Extremism can be the province of state or nonstate actors…Violent extremism is the belief than an in-group’s success or survival can never be separated from the need for violent action against an out-group (as opposed to less harmful acts such as discrimination or shunning). A violent extremist ideology may characterize its violence as defensive, offensive, or pre-emptive.”

Neither Midlarsky’s nor Berger’s definitions made a special reference to the definition of religious extremism which, arguably, has some peculiar characteristics. I therefore tried to fill this void, coming up with this definition of religious extremism:

“The pursuit, usually by a fanatical sect or cult, but occasionally also by a political ‘party of God’, a terrorist organization, or an official ‘religious establishment’ of a program of societal renewal which usually involves some form of social cleansing. The use of violence is justified by reference to a divine authority, an absolute truth, or a literal interpretation of texts deemed sacred. Specific groups of people such as non-believers, pagans, apostates or heretics are identified as enemies and as such earmarked for being subjugated, punished, expelled or killed in the name of one or
another sacred cause. Religious extremists want to purify the world from alleged forces of evil and establish a theocratic regime run by a religious leader or council. True believers who adhere to such a religious ideology tend to be prepared for martyrdom (suicide) operations, often expecting great rewards in afterlife for their sacrifice.”

Religious terrorism, with its fanaticism and being based on the conviction of its believers that martyrdom operations will be rewarded with a place and special pleasures in paradise is especially hard to prevent. One way to counter it is to promote a culture of moderation in religion as well as in politics – in other words: upstream prevention.

The prevention of extremism in politics presupposes clarity on non-extremism and on the opposite of extremism – moderation. Strangely enough, little attention has been paid to the conditions for the presence and flourishing of political moderation which, by definition, can, if successful and pervasive in society, prevent political extremism. An exception are the writings of the political scientist Aurelian Craiutu. Based on his work, moderation in politics can be said to involve ten rules of conduct:

1. Moderates have a commitment to civility in dealing with all parties in the political arena;
2. Moderates are skeptical of ideologies and oppose ideological and religious intransigence; they acknowledge that no single party is in possession of absolute truth or has definitive solutions for society’s problems;
3. Moderates are flexible and open-minded, willing to look at all sides of a divisive political issue before taking a position;
4. Moderates accept the existence and legitimacy of a plurality of viewpoints in multicultural societies, are opposed to polarizing policies, and do not wish to silence legitimate voices;
5. Moderates are bridge-builders: they search for common ground in political controversies and seek to balance and harmonize the interests of opposing political parties and social forces through dialogue, negotiation, and compromise, aiming for conciliation wherever that is possible;
6. Moderates are opposed to violent confrontation and prefer reform to revolution;
7. Moderates, in an effort to preserve and re-establish social harmony, seek to keep lines of political dialogue open and reach out for political opponents in an effort to come closer to a consensus;
8. Moderates are practical, pragmatic, flexible, rational and prudent when determining the most appropriate course of action and seeking realistic solutions;
9. Moderates are opposed to fanaticism, zealotry and extremism;
10. Moderates are tolerant – but know that tolerance is counter-productive when confronted with those who are intolerant and intransigent.

If one manages to strengthen the forces of moderation in state and society, at home and abroad, one automatically weakens the forces of extremism, provided one sticks to the last, somewhat paradoxical, tenth rule - one cannot be tolerant against the intolerant without digging one’s own grave. The cultivation of moderation in politics then, is a major form of upstream prevention of extremism.

Prevention of extremism as a way to prevent terrorism has been paralleled to some extent by efforts to prevent radicalization. The basic underlying idea is the same - as terrorism presupposes the existence of extremism, in this alternative framework it presupposes a prior
radicalization before seemingly peaceful people turn to one form of political violence called terrorism.

**Terrorism Prevention as Prevention of Radicalization**

The term radicalization was hardly used before 9/11. It was the Dutch intelligence service AIVD which introduced it in connection with countering terrorism. The concept gained traction after Al-Qaeda’s bomb attacks on trains in Madrid on March 11, 2004 (causing 191 deaths and around 2,000 injured) and has become a key concept in European official circles in the fighting against terrorism. The term “Radicalization” allowed a discussion of the causes of terrorism that put the blame for terrorism on vulnerable individuals who had allowed themselves to be attracted, mobilised and recruited by professional jihadist veterans or who were apparently self-radicalizing under the influence of terrorist propaganda distributed by social media.

The European Commission defined radicalization in 2004 as,

> “Individuals or groups becoming intolerant with regard to basic democratic values like equality and diversity; as well as a rising propensity toward using means of force to reach political goals that negate and/or undermine democracy.”

If one takes this definition literally, radicalization to terrorism only takes place in democracies. In 2016, the European Union came up with a formulation that did not contain this reference to democracy. Yet it still remains vague:

> “The EU firmly believes in eradicating terrorism at its source. Therefore, preventing terrorist attacks by addressing and stopping terrorist radicalization and recruitment is a priority for the EU, as outlined in the EU Internal Security Strategy in Action. Radicalization in this sense is understood as a complex phenomenon of people embracing radical ideology that could lead to the commitment of terrorist acts.”

This formulation is circular in that radicalization is explained in terms of people embracing radical ideology. The irony is that European democracies owe much to 19th century radical ideologies and the movements and political parties which were inspired by ideas of the 18th century Enlightenment with its idea of progress and the emancipation of common people. Ideas like the right to vote for all men (not just those who possessed property) as well as women, separation of church and state and republicanism rather than monarchism were typical political demands of radical parties. Those 19th century radicals were fighting for democracy and we owe much to the struggle of radical suffragettes and others who helped to bring democracy to the common men and women.

Questionable as a direct linking of radicalization to radicalism is in terms of the history of ideas, the term radicalization has gained such widespread currency that it is unlikely to disappear. I therefore tried in 2013 to re-conceptualize radicalization in a way that is more balanced:

> “An individual or collective (group) process whereby, usually in a situation of political polarization, normal practices of dialogue, compromise and tolerance between political actors and groups with diverging interests are abandoned by one or both sides in a conflict dyad
in favour of a growing commitment to engage in confrontational tactics of conflict-waging.

These can include either (i) the use of (non-violent) pressure and coercion; (ii) various forms of political violence other than terrorism; or (iii) acts of violent extremism in the form of terrorism and war crimes.

The process is, on the side of rebel factions, generally accompanied by an ideological socialization away from mainstream or status quo-oriented positions towards more radical or extremist positions involving a dichotomous world view and the acceptance of an alternative focal point of political mobilization outside the dominant political order as the existing system is no longer recognized as appropriate or legitimate."

With the help of such a reconceptualization, it becomes possible to look at radicalization not just at the individual micro-level but also at the group and societal meso-level and at structural factors linked to the state and the international system (macro-level). It allows us to go beyond the one-sided use of the term radicalization for non-state actors only and also breaks the direct link between radicalism and radicalization. Radicalization does not have to end in violence when pushed to extremes; it can also become a force for good as has recently been pointed out in the award-winning dissertation by Ken Reidy “The Accidental Ambassadors: Implications of Benevolent Radicalization.” He showed that one may radicalize in a malevolent manner (resulting in terrorism and/or extremism) but also in a benevolent manner (resulting in becoming a voluntary humanitarian aid worker in the same war zones that also attract foreign fighters).  

While this is a useful expansion of the concept of radicalization, most studies on radicalization and its prevention have a narrow focus that is insufficient to explain and tackle terrorism in all its forms and manifestations. The link between radicalization and terrorism, and even more so, between radicalism and terrorism is not always direct and sometimes totally absent.65

**Analytical Framework for Exploring Terrorism Prevention**

For the purpose of this *Handbook of Terrorism Prevention and Preparedness*, the editor – after receiving feedback from some other contributors to this volume – proposed the following typology related to terrorism prevention and preparedness.

Terrorism prevention can be broken down into taking pro-active, precautionary measures at three moments in time:

- **Upstream, primary (early) prevention:** reducing the risk of the formation of a terrorist group or organization,
- **Midstream, secondary (timely) prevention:** reducing the risk of such a group or organization being able to prepare a terrorist campaign and
- **Downstream, tertiary (late) prevention:** reducing the risk of execution of individual terrorist operations by foiling and deterring these.

In other words, if terrorist group formation cannot be forestalled in an early phase by taking appropriate upstream measures, the focus should be on preventing the preparation of terrorist campaigns and, if that also fails, prevention should seek to obstruct the occurrence of individual terrorist attacks.
Based on these considerations, the editor of this volume suggested to the contributors of the various chapters the following working definition of “Terrorism Prevention and Preparedness:”

**Prevention of terrorism** involves the anticipation of risk factors giving rise to terrorist group formation, terrorist campaign initiation and/or specific attack preparations and responding to these by:

**Preparedness**, that is, taking proactive and preemptive measures to reduce risks and threats and, if that turns out to be insufficient, reduce the negative impact of terrorist attacks through a set of planned precautionary measures aimed at strengthening governmental readiness and societal resilience.66

For each of these three phases (upstream, midstream, downstream), a number of preventive actions can be taken. The examples provided below are illustrative rather than comprehensive and systematic.

**Upstream Terrorism Prevention**

When the editor of this Handbook was working for the United Nations as Officer-in-Charge of the Terrorism Prevention Branch of the UN Office on Drugs and Crime (UNODC) at the beginning of this century, he proposed four upstream measures for terrorism prevention, arguing that these should be the four pillars on which successful preventive national anti-terrorism measures should built.67

Upstream prevention on the national level:

- **Good Governance**, because when governance is bad, resistance against corrupt rule gains followers and support and might take the form of terrorism;
- **Democracy**, because when unpopular rulers cannot be voted away by democratic procedures, advocates of political violence find a wider audience;
- **Rule of Law**, because when rulers stand above the law and use the law as a political instrument against their opponents, the law loses its legitimacy and credibility, and encourages people to turn to alternative normative systems;
- **Social Justice**, because when long-standing injustices in society are not addressed but allowed to continue for years, without any light in sight at the end of the tunnel, desperate people, and some others championing their cause, are willing to die and to kill for what they perceive to be a just cause.68

This short list of upstream drivers addressing situations that might act as triggers encouraging the formation of terrorist groups/organizations found later some statistical confirmation in social science research by the University of Maryland’s START project that looked at the correlations of terrorism.69

Given the communicative purpose of terrorist performances, other crucial upstream drivers of terrorism are mass media and, more recently, social media, since they offer non-state terrorists the opportunity to make their agitation and propaganda tactics work. Yet another upstream driver for some forms of terrorism is religion, or rather, some manifestations of religion as currently witnessed most strongly by the fanaticism among certain Salafist sectors of Sunni Islam. Another major upstream driver is armed conflict (insurgency and counterinsurgency at home and armed interventions, overt and covert, abroad, often accompanied by military occupation). This usually provokes rebellion and resistance, partly manifesting itself in acts of terrorism.
Given the increasingly transnational nature of terrorism, national preventive measures are of limited use when major drivers of the problem are abroad and migration, porous borders and internet-based communication and radicalization come into play. Therefore, upstream prevention has also to address, difficult as it is, foreign drivers such as these:

- **Address conflict formations and sources of conflict perpetuation abroad** by offering to mediate between government and opposition groups to avoid further bloodshed and conflict escalation;
- **Contribute to UN and regional peace-keeping and peace-building efforts** to reduce the operational territory of armed non-state groups in weak and failed states;
- **Counter cross-border financing of terrorism** by investigating and blocking sources of income of terrorist groups;
- **Strengthen moderate civil society actors abroad** against religious and other fanatics.

Globalization has helped to make terrorism near global while counterterrorism and preventive measures across borders have been lagging behind.

Where it is not possible to effectively address upstream drivers that can lead to the formation of terrorist groups and organizations, enhanced emphasis has to be placed on midstream measures.

**Midstream Terrorism Prevention**

When it comes to midstream terrorism prevention, an important role relates to deficient socialization and education of young people in their own immediate surroundings, especially when children are exposed to violence at home. Domestic violence within the family rarely stays at home but, sooner or later, often tends to spill over into society. Since nobody is born a terrorist, push and pull factors during adolescence and acts of commission and omission from parents, schools, and communities during the formative years of a child play a large role in turning young people to harmful and problematic behaviors when the immediate environment cannot satisfy the basic human needs of young people.

Experience with, and exposure to, violence in early life tends to produce, if untreated, lifelong traumas and can also lead to new cycles of violence which, in most cases, are not terrorist in nature but relate to crime and violence as well as mental health problems in general. In order to prevent young people from becoming attracted to harmful forms of pseudo self-actualization (namely, drug and alcohol abuse, joining a youth gang involved in crimes, escapism into the virtual world of violent internet games, joining religious sects, or becoming part of militant extremist groups engaged in acts of terrorism at home or abroad), a number of midstream preventive measures should be put in place:

- Providing parents with infrastructures and opportunities that allow them to take good care of their children until they can stand on their own feet;
- Providing young people with affordable and good quality education to learn skills and develop their talents so that they can find their place in society;
- Offering young people challenging extra-curricular activities to keep them away from criminal gangs or religious sects;
- Provide young people with formal and informal opportunities to engage with the opposite sex in a responsible and respectful way;
- Facilitate cultural exchanges to allow young people to learn about, and tolerate, other ways of life.

If young people are neglected and/or abused, they will seek unhealthy opportunities for self-actualization. Much can be done to prevent this. However, rather than subsuming this under labels like radicalization prevention, it is better that it should fall under general
prevention in the form of, for instance, positive parenting initiatives such as: kindergarten (nursery school) initiatives for extra-family socialization; school-based programs emphasizing fair play, empathy and solidarity; community-based programs enhancing integration and social cohesion; providing young people with positive role models via alternative media; and opening up real avenues for upward social mobility for young people through education and civil service programs for those who cannot otherwise find their place in society.71

Midstream terrorism prevention should be broader and involve elements such as community policing and other measures - not just focusing on “vulnerable individuals” but also on neglected neighbourhoods with high levels of unemployment and ill-assimilated immigrant diasporas exposed to discrimination and humiliation. The goals should be broader than simply focusing on the prevention of radicalization and recruitment by terrorist cells eager to prepare a terrorist campaign. A broader approach of better caring for youth has other benefits such as crime reduction and fewer mental health problems in society.

**Downstream Terrorism Prevention**

When one thinks of terrorism prevention, what first comes to mind are downstream preventive measures - such as not allowing guns and explosives to be brought on board of commercial airliners. Below are a number of typical measures that can be taken downstream.72 Again, this list has only illustrative character and applies only to certain types of terrorism but not others. In this sample, measures are divided into passive and active measures.

**Passive Prevention**

- Gun and explosive materials detection instruments at airports;
- Border and travel documents controls (including entry and exit control systems);
- Deterrence: threatening retaliation and punishment;
- Target hardening (e.g. using bomb blast resistant window films)

**Active Operational Tactical Prevention**

- Surveillance of suspects and bugging of their homes, cars, and meeting places;
- Neutralization through infiltrations into terrorist groups;
- Prevention through entrapment of extremists suspected of being on the point of preparing acts of terrorism;
- Preventive detentions or house arrests of dangerous extremists, based on court orders.

Tore Bjørgo distinguishes between “long-term preventive strategies” and “short-term preventive strategies.” Some of the latter overlap with the downstream measures listed above:

- Deterrence by threat of retaliation or punishment;
- Pre-emptive disruption of planned terrorist attacks;
- Incapacitation;
- Protecting vulnerable targets.73

Should upstream, midstream and downstream prevention fail, mitigating measures ought to be in place to reduce the impact of terrorist attacks through contingency planning and preparedness led by a governmental response-and-recovery apparatus that is geared to reduce harm and also serves to strengthen societal resilience.74
Conclusion

As the experience of the last two decades has made clear, it has proven difficult to de-radicalize terrorists and to counter violent extremists. This has led to a certain bifurcation of anti-terrorism in recent years. On the one hand, there has been a return to a hardline armed response to counterterrorism and, on the other hand, a renewed interest in the prevention of terrorism, sometimes in the form of prevention of radicalization and at other times in the form of prevention of extremism.

In this volume, we adhere to the concept of terrorism prevention, although we recognize the importance of preventing radicalization and extremism since these are partly co-extensive with the object of investigation here. A major reason for adhering to terrorism prevention is that the alternative terms, radicalization and extremism, are even less well defined than terrorism, the first one being too narrow and the second one being too broad. Current efforts at the prevention of radicalization are focusing too much on the individual level, while efforts to prevent violent extremism focus too much on the ideological level, while at the same time often excluding certain state-sponsored religions as drivers. However, if radicalization is re-conceptualized as suggested earlier in this chapter, it can provide a framework that goes beyond the “vulnerable individual” and also enables us to see positive sides to radicalization, namely when it is benevolent rather than malevolent, and “activist” but not “terrorist” in nature. When it comes to extremism, the widely used distinction between violent and non-violent extremism is of dubious value since it has nothing to do with classical non-violence in the tradition of Mahatma Gandhi or Martin Luther King Jr. The opposite of all extremism is moderation and the prevention of extremism ought to take the form of strengthening moderation in both politics and religion.

Prevention is a difficult field of study because it is based on the anticipation of a future that is impossible to know with certainty. In this sense, terrorism poses a “wicked problem.” A “wicked problem” has been defined as

“.... a social or cultural problem that is difficult or impossible to solve for as many as four reasons: incomplete or contradictory knowledge, the number of people and opinions involved, the large economic burden, and the interconnected nature of these problems with other problems.”

There is no simple, clear-cut solution to wicked problems. Modern non-state terrorism has been around for 150 years and while the level of attacks has waxed and waned, terrorism is highly unlikely to ever go away. Complete prevention is impossible short of closing down open societies and sealing borders but preventive measures can have measurable effects over time – there are no quick fixes. A better understanding of the problem of terrorism and its prevention, however, is within our reach once we have some basic agreement about the exact object of prevention and greater clarity about the methods to bring this about. The conceptual discussion of this chapter has sought to contribute to this and encourage the contributors of this Handbook to further elaborate new approaches to the problem and suggest better ways to address it.

Alex P. Schmid is a Research Fellow at the International Centre for Counter-Terrorism (ICCT) in the Hague, the Netherlands. He is Editor-in-Chief of Perspectives on Terrorism and former Co-Editor of Terrorism and Political Violence – both leading journals in the field of Terrorism Studies. Until 2009, Prof. em. Schmid held a chair in International Relations at the University of St. Andrews where he was also Director of the Centre for the Study of Terrorism and Political Violence (CSTPV). Previous positions include Officer-in-Charge of the Terrorism Prevention Branch of the UN Office on Drugs and Crime in Vienna and a chair in Conflict
Resolution at the Erasmus University Rotterdam. Between 1978 and 2018 he also held various positions at Leiden University. Currently, he is Director of the Vienna-based Terrorism Research Initiative (TRI), a consortium of 16 institutes and more than 100 individual scholars seeking to enhance human security through collaborative research. Alex Schmid has more than 200 publication and reports in ten languages to his name, including the award-winning volume “Political Terrorism” (1984, 1988, 2006) and the “Routledge Handbook of Terrorism Research” (2011, 2013).
Appendix I

Selected Definitions of Prevention with Regard to Conflict, Crime, Extremism, Radicalization, Terrorism, Violence

“Nowhere is there agreement about quite what prevention is, while everywhere there is agreement that it is a good thing.”

R. Freeman, 1992

Conflict prevention (Schmid, 2000): A broad concept which refers to anticipation and aversion of escalation and violence in social, political and international conflicts. It covers:

A. Primary prevention (minimizing chance of occurrence of violent conflict):
   1. Proactive measures to prevent the emergence of conflict formation between parties; and
   2. Prophylactic measures to prevent the likely outbreak of a conflict between parties.

B. Secondary prevention (containment and mitigation):
   1. Active measures to prevent the vertical escalation of existing conflicts;
   2. Reactive measures to limit horizontal escalation of already on-going conflict to other areas; and
   3. Palliative measures to mitigate the consequences of an outbreak of conflict.

C. Tertiary prevention (preventing the recurrence of armed conflict):
   1. Revalidation measures aimed at preventing the renewal of the conflict cycle in the post-conflict phase.

Crime prevention (US National Crime Prevention Institute, 2001): “The formal definition of crime prevention as adopted in several countries is: the anticipation, recognition, and appraisal of a crime risk and the initiation of some action to remove or reduce it.”

Crime prevention (United Nations, 2002): “...is defined as comprising all measures that seek to reduce the risk of crime occurring by intervening in its multiple causes.”

The [UN] guidelines distinguish four main categories of crime prevention:

1. Social crime prevention, including early intervention
2. Community-based crime prevention
3. Situational and victim-oriented crime prevention
4. D. reintegrating offenders.

“For the purposes of the present guidelines, “crime prevention” comprises strategies and measures that seek to reduce the risk of crimes occurring, and their potential harmful effects on individuals and society, including fear of crime, by intervening to influence their multiple causes. The enforcement of laws, sentences and corrections, while also performing preventive functions, falls outside the scope of the Guidelines, given the comprehensive coverage of the subject in other United Nations instruments.”

Prevention (Schmid, 2011): “The taking of long-term proactive measures to remove the causes of an undesirable development or to obstruct the occurrence of an unwanted situation; social and technical engineering to reduce individual or collective harm or damage by
inhibiting, dissuading or deterring potential offenders, also by creating environments where criminal activity is made more difficult (situational crime prevention).”82

Crime prevention (Oxford Handbook of Crime Prevention (2012): “Crime prevention has come to mean many different things to many different people. In one of the first scholarly attempts to differentiate crime prevention from crime control, Peter Lejins espoused the following: ‘If societal action is motivated by an offense that has already taken place, we are dealing with control; if the offence is only anticipated, we are dealing with prevention’ Crime prevention is best viewed as an alternative approach to reducing crime, operating outside the formal justice system. Developmental, community, and situational strategies define its scope. Developmental prevention has emerged as an important strategy to improve children’s life chances and prevent them from embarking on a life of crime Community crime prevention benefits from a sound theoretical base….The theoretical origins of situational crime prevention are wide ranging and robust.”83

Violence prevention (World Health Organization, 2014): “…violence can be prevented. Interventions to address violence are delivered as part of a four-step public health approach that includes 1) defining the problem; 2) identifying causes and risk factors; 3) designing and testing interventions, and 4) increasing the scale of effective interventions.”84

Radicalization and extremism prevention (Austrian government, 2018): “In the context at hand, prevention refers to the identification and conception of strategies and measures which aim at containing the risk of radicalization and extremism.”85

Terrorism prevention (RAND, 2019): “…for the purposes of our work, we constructed a baseline definition that drew on elements from definitions in the literature and from discussions with interviewees:

“Terrorism prevention policy seeks to reduce the incidence of violence inspired by ideology and extremist causes, and to expand the range of options for responding to that risk. It includes efforts – either alone or in collaboration – by such government entities as law enforcement, social services, and mental health agencies; non-governmental organizations; civil society; community groups; and the private sector.

By building options beyond the traditional criminal justice tools of arrest, prosecution, and incarceration – and involving organizations and capabilities outside the organizational boundaries of government – terrorism prevention programs seek to enable action earlier, before individuals have taken illegal actions that could pose imminent danger and have lasting consequences both for themselves and others.”

Our definition focuses specifically on violence rather than beliefs because individuals’ freedom of beliefs, religion, and political views is protected”. Terrorism prevention policies and programs are aimed at reducing the risk of terrorism in ways other than investigating and incarcerating the individuals suspected of planning or directly supporting violence. The tools for doing so span the entire life cycle of terrorism, from preventing recruitment by terrorist groups to limiting the influence of terrorist messaging to intervening with individuals who are at risk of radicalization to violence. Such tools also include programs to preclude recidivism for those incarcerated for terrorist-related violence.”86
Appendix II

A Note on Prevention by Removing Root Causes of Terrorism

We like to think in terms of cause and effect and often assume that by removing the cause we can prevent the – in our case – unwanted effect, namely terrorism. Unfortunately, it is not that easy. It has not been easy either in other areas of prevention (e.g., the prevention of crime, war, or cancer).

Why is this so? To begin with, a cause can have several effects, some desirable and others not, and the price of preventing one undesirable effect – terrorism in our case – among many more desirable ones is a price that one might not be willing to pay. On the other hand, one single effect may have more than one cause.

A second problem is that there are many definitions of terrorism and depending on how this contested term is defined, the causes are also likely to differ. Then there are also many types of terrorism – from ‘lone wolf’ terrorism to ‘cyber-terrorism’ – and different forms of terrorism also tend to have different causes.

If we look at the vast literature on terrorism as well as at statements on terrorism made by terrorists, politicians, and other influencers, we find a bewildering variety of alleged root causes. Some are broad and general, others narrow and specific. Many have not been tested and are in fact empirically untestable because these alleged “causes” are too vague. Some have been proven wrong (e.g. poverty as cause) but are still turning up in political rhetoric. Others are only contributing factors to the emergence of terrorism under specific circumstances. Some “root causes” might be necessary but are not sufficient conditions.

Here are a number of causal factors which can be found in the media and in academic and other journals. For brevity’s sake, a source is only specified for the last example.

Alleged Root Causes, Pre-conditions, and Contributing Risk Factors Associated with Terrorism

Globalization; rapid modernization; Western alliances with Middle Eastern dictatorships; foreign intervention and/or occupation; unjust world order; failed or weak states; lack of freedom and democracy; oppression and repression; illegitimate or corrupt governments; violation of basic human rights; growing racial or social inequality; ethnic or religious discrimination; ethnic diversity; social polarization; feelings of injustice; extremist ideology; mental illness; radicalization in prisons or refugee camps; alienation; grievances; political discontent; frustration about absolute or relative deprivation (e.g., poverty); unemployment; youth bulge; ideological radicalization; desire for revenge, retribution, punishment; desire to (re-)gain sense of significance; desire to dramatize injustices and create impetus for reform; Alienation from, and discrimination in, host country; rage in response to humiliation; feelings of powerlessness and deprivation; feelings of marginalization and exclusion; disillusionment over impossibility of bringing about change by other means; bitter hopelessness and desperation, with terrorism being weapon of last resort; ideological radicalization to extremist ideology; desire for national self-determination; instrument to accelerate “history”; tool to reinstate, reinforce supremacy of own group; no other choice (weapon of the weak); absence of alternative channels of influence; to obtain access to mass media (propaganda of the deed); to unblock blocked society (no democratic change possible); to press for solution in unresolved conflict; tactic of provocation to trigger repression that will bring new recruits; easy availability of targets and weapons in open democratic societies; shortcomings in preventive measures; weak border/perimeter controls allowing access to targets; mimetic urge to do likewise
(contagion); outcome of a learning process; fanaticism; religious duty rewarded by place in paradise; defense of the community (Ummah); defense of the prophet; divine command.

Clearly, many of these “causes” are difficult if not impossible to remove (e.g., the last one: divine command). Like in the case of (non-political) crimes, the spectrum of the phenomenon of (political) terrorism is wide, especially if one not only looks at the means (stabbing, shooting, assassination, IED bombing, hostage taking, hijacking, suicide attacks, vehicle ramming attack etc.) but also at the multiple ends, motives and intentions which are often hard to separate. All this makes the prevention of terrorism a difficult and complex task.
Endnotes


3 Ibid., p. 7.


6 Peeters 2013, p. 7.

7 Gough 2015, p. 3.


9 CVE has, in the US context, for lack of an official definition, been defined by Caitlin E. Ambrozik as “a collection of non-punitive policies and programs that aim to either prevent violent extremism and disrupt an individual or group’s reliance on violent extremism by attempting to address the root causes of violent extremism… In practice, there are four main components that practitioners and scholars typically associate with CVE: prevention, intervention, deradicalization, and disengagement. Each component can include a variety of different programs that operate in the non-criminal or criminal spaces of public policy.” Ambrozik, Caitlin E., *Countering Violent Extremism Locally.* Ithaca, NY: Cornell University, 2018, p. 3.


16 Radicalism, in the European tradition, was, in the 19th century, situated ideologically between socialism and liberalism and is rooted in the 18th century enlightenment and linked to the idea of progress and the emancipation of the underprivileged. Radicalism differs from extremism which is supremacist rather than egalitarian, rejects pluralism and denies human rights to members of the out-group.
19 What is omitted here is a discussion of the literature on the prevention of violence and aggression, which is very extensive, ranging from prevention of bullying to prevention of nuclear war.
24 Despite serious shortcomings, this draft definition has been left unchanged for many years as the members of the Ad Hoc Committee quarrel over some of the other 27 paragraphs of the draft for a Comprehensive Terrorism Convention - mainly those dealing with the scope of the convention (should it also apply to the armed forces of UN member states? And should the activities of non-state “parties” (e.g. Hamas) fighting for “national liberation” be excluded from the application of the convention?). For a discussion, see: Schmid, Alex P. (ed.), *The Routledge Handbook of Terrorism Research.* London and New York: Routledge, 2011, pp. 50-60; and Saul, Ben, ‘Defining Terrorism: A Conceptual Minefield’; in: Chenoweth, Erica et al. (eds.), *The Oxford Handbook of Terrorism.* Oxford: Oxford University Press, 2019, pp. 34-49. See also Margariti 2017, pp. 159-166.
25 Schmid 2011, pp. 86-87. For a fuller version of the Academic Consensus Definition, see the online journal ‘Perspectives on Terrorism,’ 6(2), 2012. Available at: https://www.universiteitleen.nl/perspectives-on-terrorism. For an expanded explanation, see Schmid, Alex P., ‘The Definition of Terrorism’; in: Schmid, Alex P. (ed.), *The Routledge Handbook of Terrorism Research.* London and New York: Routledge, 2011, pp. 39-98 and the Appendix 2.1: ‘250-plus Academic, Governmental and Intergovernmental Definitions’. Earlier the author of this academic consensus definition had also suggested a legal definition to the UN which was, however, not accepted. He had proposed, in 1992, to extend the uncontroversial definition of ‘war crimes’ from war times to peace times, defining acts of...


29 Ibid., p. 258.


32 There are ten main audiences: 1) adversary(-ies) – usually government(s); 2) society of the adversary(-ies); 3) direct victims and their relatives and friends; 4) others who have reason to fear that they might become targets; 5) members and supporters of terrorist organizations; 6) other rival terrorist or political party organizations; 7) constituency terrorists claim to represent/act for the terrorist/terrorist group; 8) potentially sympathetic sectors of domestic and foreign (diaspora) publics; 9) ‘neutral’ distant publics which have not (yet) taken sides; and last, but not least; 10) the media. By the way, the terrorist audience can also be the terrorist him or herself – a perverse form of self-glorification.


34 Schmid and de Graaf, 1982.


37 Gough 2015, Table 1. Varying definitions of primary, secondary and tertiary forms of prevention.

38 Jackson et al. 2019, p. 40 (Figure 3.1. Radicalization and Mobilization States, with Phases of Terrorism Prevention).


40 Gough 2015, Table 1.

41 The Danish model of extremism prevention evolved from a pilot model developed in the city of Aarhus to counter radicalization in 2007. By 2014, it had become Denmark’s nationwide approach and since then it has become an often-cited example for other European countries. See Nationalt Center for Forebyggelse af Ekstremisme, *Knowledge Synthesis. Mapping of Knowledge on Extremism and Prevention of Extremism*. Copenhagen, 2018, p. 39. Available at: https://stopekstremisme.dk/en/prevention.


Bjørgo 2013, p. 5.

Bjørgo, Tore, ‘Strategies for preventing violent extremism and terrorism,’ Oslo: C-REX, n.d. (powerpoint presentation, slide 5). Also in Bjørgo, Tore, *Preventing Crime: A Holistic Approach*. Basingstoke: Palgrave Macmillan, 2016. It should be noted that the wording has changed slightly between 2013 and 2016 in his work. In Bjørgo’s conceptualization, “preventive mechanisms” refer to how do these mechanisms reduce (future) acts of terrorism, while measures refer to the instruments used to activate these mechanisms. For instance, when it comes to mechanisms to reduce radicalization and recruitment to terrorism and violent extremism, the recommended measures are conflict resolution, political processes, social development, non-discrimination, rule of law, social work, etc. See Bjørgo, Tore, ‘Strategies for preventing violent extremism and terrorism,’ Oslo: C-REX, n.d. (powerpoint presentation, slide 7).

Passage taken from Foreword by Alex P. Schmid to Bjorgo’s volume (p. viii).

Ambozvik 2018, p. 3.


56 Berger 2018, pp. 44-46.
57 Presentation by Alex P. Schmid, 25 May 2018, the Centre for Research on Extremism (C-REX) Oslo.
63 Schmid 2013.
65 Schmid 2013.
66 This definition is based on a number of sources, including those cited in the appendix, e.g.: National Crime Prevention Institute (USA), Understanding Crime Prevention. Woburn, WA: Butterworth-Heinemann, 2001, p. 3. One definition of crime prevention adopted by several countries is “the anticipation, recognition, and appraisal of a crime risk and the initiation of some action to remove or reduce it.” Tore Bjørgo uses the term prevention to refer to “….reducing future acts of terrorism or other crimes, or reducing the harmful consequences of such acts, by proactive measures.” See Bjørgo 2013,p.5. See also: the glossary in Schmid 2011, p. 676.
68 Ibid. Wording slightly modified here.
69 The START study, ‘Correlates of Terrorism,’ based on the Global Terrorism Database of the University of Maryland, which by now includes over 190,000 incidents (150,000 in 2011) found in 2012 that higher levels of terrorism were strongly associated with the following factors: 1) higher levels of group grievances; 2) lower levels of intergroup cohesion; 3) higher levels of organized conflict; 4) higher levels of political (state) violence; 5) lower human rights standards; 6) higher numbers of refugees and internally displaced people; 7) lower levels of political stability; 8) lower levels of negative peace, and (ix) lower levels of internal peace. START, Global Terrorism Index 2012. College Park: University of Maryland, 2012, p. 34. See also Parker, Tom, Avoiding the Terrorist Trap. Why Respect for Human Rights is the Key to Defeating Terrorism. New Jersey: World Scientific, 2019. See also the chapter by McAllister, Bradley and Alex P. Schmid, ‘Theories of Terrorism’; in: Schmid, Alex P. (ed.), The Routledge Handbook of Terrorism Research, New York and London: Routledge, 2011, pp. 201-279.


A Danish literature survey noted in 2016, “it must be emphasized that researchers and practitioners do not have a collective understanding of the terms radicalization and extremism.” Nationalt Center for Forebygglse af Ekstremisme, 2016, p.6.


Survey of the Literature on Terrorism, by Brynjar Lia (pp.276-279). Other causal factors are from the chapter “Theories of Terrorism” by Bradley McAllister and Alex P. Schmid in the same volume (pp.201-271). Additional “causes” are from Goodwin, Jeff, ‘The Causes of Terrorism’ in: Chenoweth, Erica et al. (eds.), *The Oxford Handbook of Terrorism*. Oxford: Oxford University Press, 2019, chapter 17, pp. 253-267. The first seminal study on causes was Crenshaw, Martha, ‘The Causes of Terrorism,’ *Comparative Politics*, 13 (4), 1989, pp. 379-399.

Bibliography


Barbash, Fred, ‘Boko Haram leader Abubakar Shekau claims massacre was command from God,’ The Sidney Morning Herald, 22 January 2015.


Schmid, Alex P., ‘Violent and Non-Violent Extremism: Two Sides of the Same Coin?’ The International Centre for Counter-Terrorism - The Hague (ICCT), 2014. Available at: http://dx.doi.org/10.19165/2014.1.05.


Web-based Resources

Deutscher Präventionstag, Islamismus und Terrorismus – Möglichkeiten der Prävention. Available at: https://www.praeventionstag.de/nano.cms/vortraege/id/134.


Society for Prevention Research. Available at: www.preventionresearch.org

Scrivens, Ryan, Theses (Ph.D. and MA) on CVE, PVE and TP, Perspectives on Terrorism, 6(2), February 2019. Available at: https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2019/issue-1/scrivens.pdf.


US National Criminal Justice Reference Service: 500 title on ‘Terrorism Prevention’. Available at: https://www.ncjrs.gov/App/AbstractDB/AbstractDBSearchResults.aspx?Title=&Author=&Journal=&NCJNum=&General= Terrorism+Prevention&StartDate=&EndDate=&SearchMode=All&fromTopics=&SortBy=2&Offset=0&SelectedRange=init&SelectedSearchItems=init
This chapter provides an overview of the ways in which criminology and the crime prevention literature have contributed, and might prospectively contribute, to the study and practice of terrorism prevention. Underlying the discussion is the critical premise that terrorism is, inexorably, a particular form of crime, and that criminological perspectives accordingly function as key components of any comprehensive strategy for terrorism prevention and preparedness. Models and foundational concepts in crime prevention are introduced with a focus on situational crime prevention and its theoretical underpinnings. The application of situational crime prevention (SCP) to terrorism prevention is traced from its promising point of departure in 2006 through its evolution up to the present time. In addition, crime prevention models outside of (or extending beyond) situational crime prevention are considered to afford a broader overview of the maturing criminological perspective on terrorism prevention. Finally, benefits and drawbacks of the foregoing approaches are considered and directions for possible future research are discussed.

Keywords: crime, crime prevention, criminology, terrorism, situational crime prevention
A substantial and growing body of literature applies a criminological framework to the challenges of terrorism prevention. Although other disciplines, including political science and psychology, have played more dominant roles in the development of terrorism studies, criminology and crime prevention literature increasingly lend a critical perspective that complements approaches based in other social sciences. A rigorous crime prevention approach also provides a pragmatic counterbalance to more reactive national security approaches. Strategies derived from crime prevention thus help to address the widening recognition that militarized and repressive measures alone cannot provide the most effective counterterrorism strategies for the long run, rather, a complement of more preventive and constructive approaches is needed.

Crime prevention approaches to terrorism rest on the recognition that terrorism is indeed a particular and egregious form of crime, prohibited (along with its manifestations such as murder and kidnapping) by laws across jurisdictions, and can be addressed fruitfully as such. Within criminology, the crime prevention literature is not monolithic, but employs contrasting perspectives and models. Prominent among these are the social crime prevention (SCP) model, the situational crime prevention model, and the criminal justice model (CJM). Some frameworks essentially parse social prevention into two components – developmental and community prevention – while still recognizing the contributions of situational crime prevention and law enforcement. An alternative conceptualization, rooted in public health literature, classifies crime prevention approaches into primary, secondary, and tertiary levels of prevention. Finally, Tore Bjørgo (2013) offers a nine-point model for crime prevention that combines key elements from the previous approaches into one novel and comprehensive formulation. Each of these approaches merits exploration in terms of its actual and/or potential contribution to terrorism prevention.

In particular, SCP-related factors neatly fit into the literature relating to terrorism prevention, and therefore this overview highlights the SCP approach in the greatest detail as well. SCP applies knowledge of criminal patterns to remove or diminish opportunities for potential perpetrators to commit specific crimes. In the counterterrorism context, SCP aims to prevent specific forms of terrorism by changing environmental circumstances, rather than changing individual terrorists and their particular dispositions. Clarke and Newman’s seminal book from 2006, titled *Outsmarting the Terrorists*, provides a point of departure. The authors persuasively demonstrate the application of SCP to terrorism. In the years since the publication of *Outsmarting the Terrorists*, over 60 additional published works have appeared on that topic.

Viewing and addressing terrorism through an SCP model provides a range of potential benefits in practical prevention, as well as some possible drawbacks, as discussed herein. For example, using SCP methods, authorities can both prevent attacks in some cases and reduce the harm that results from them in others. Further, addressing terrorism through the lens of SCP may lower expectations for its complete eradication, and contribute to a more balanced perception of terrorism in relation to other threats. On the other hand, a *displacement effect* may cause deterred terrorists simply to redirect their efforts toward other crimes or targets. Further, some critics view differences between terrorism and ordinary crime as highly significant, and argue that current SCP approaches lack the requisite nuance for effective prevention in a terrorism context. Overall, the crime prevention literature in general, and the literature addressing SCP specifically, have much to offer in the related field of terrorism prevention. Indeed, “[b]y focusing on the obvious connections between terrorism and crime, we may be able not only to contribute to a better understanding of terrorism, but also to help formulate more rational policies for combating it.”

The discussion and literature review that follow assess the contributions of the crime prevention literature to the prevention of terrorism to date. First, in order to lay a conceptual foundation for its application in the terrorism context, this chapter broadly describes different strands of crime prevention featuring prominently in the literature. Approaches within crime
prevention warranting attention here include social and situational crime prevention; developmental and community prevention; and the criminal justice model. The discussion proceeds to detail the principles of SCP in greater depth, tracing the application of SCP and other crime prevention models in the context of terrorism prevention. In this regard, Clarke and Newman’s groundbreaking application of SCP principles to terrorism prevention feature prominently, as do the related endeavors that followed. For example, researchers have studied the application of crime prevention principles to bioterrorism, eco-terrorism, hostage-taking, and ideologically motivated tax refusal, among many other areas. Special attention is afforded to Tore Bjørgo’s crime prevention model, as applied to terrorism prevention. Bjørgo’s model integrates key elements from the other crime prevention models discussed above, rendering them compatible and tailoring them for the context of terrorism prevention. Finally, the chapter highlights potential advantages and drawbacks of applying SCP or other criminological approaches in the context of terrorism prevention, and discusses areas for future research.

Key Concepts in Crime Prevention

Overview of the Prevention of Crime and Terrorism

Within the larger field of criminology, crime prevention offers a unique perspective and has emerged as a sub-discipline in its own right. Crime prevention refers to efforts to forestall crime or criminal offending in the first instance – before the act has been committed. While traditional vehicles for addressing crime include institutions such as police forces, courts, and corrections, broader crime prevention efforts often take place outside the formal justice system as well. Thus, crime prevention has been described as an alternative approach to the “dominant crime control model” in the United States and other Western nations, as well as an important component of an overall strategy to reduce crime.

The proactive, whole-of-society orientation of crime prevention places it squarely in line with the post-9/11 policy shift in counterterrorism toward prioritizing the prevention of terrorist acts before they occur. In the United States, this new mandate was shared across law enforcement agencies in the wake of the attacks of September 11, 2001. In an oft-cited example, the Federal Bureau of Investigation (FBI) transformed itself after the attacks, adopting a proactive approach to predicting and preventing threats before they could be realized, rather than primarily investigating terrorist crimes after they occurred.

At the same time, the 9/11 attacks and other high-profile terrorist attacks around the globe in recent decades have resulted in increased funding opportunities for, and scholarly interest in, rigorous social science-based approaches for understanding and addressing terrorism. Many of the studies flowing from the increased levels of funding and engagement have been rooted in criminology, leading to significant progress in this area. It has not escaped many scholars that terrorism prevention stands to benefit from advancements within crime prevention research, and vice versa.

Major Strands in Crime Prevention Literature

In the field of general crime prevention, experts have developed a number of wide-ranging models and typologies, extending into diverse disciplines and fields of discourse. While sometimes overlapping with each other conceptually, these models also embody partially competing perspectives. Tonry and Farrington identified four different crime prevention strategies; law enforcement on the one hand, and developmental, situational, and community prevention on the other. This four-part framework serves as a helpful tool for considering some basic foundations of crime prevention.
The law enforcement model refers to the formal institutions of criminal justice in society – i.e., police forces and prosecutors, criminal courts, and penitentiary systems. This model is sometimes understood as being focused on the preventive effects of punishment.\textsuperscript{15} In their foundational study of strategic approaches to crime prevention, Tonry and Farrington afford comparatively minimal attention to the criminal justice system, while focusing largely on the other three components of crime prevention – developmental, situational, and community prevention. Their rationale for this choice rests with the limited preventive effect of sanctions, and the conclusion shared “in most countries that have an empirical research tradition concerning criminological subjects. ...the direct marginal crime-reductive effects of foreseeable changes in the criminal law or criminal justice processes are modest.”\textsuperscript{16}

Considering the rationales that underlie the imposition of criminal sanctions in societies – and the methods used to achieve those objectives – may provide additional insights concerning the criminal justice model and its relationship to crime prevention. Within the US federal justice system, for example, the “textbook purposes” for sentencing have long been thought to include retribution, deterrence, incapacitation, and rehabilitation, with those rationales attaining different levels of respective prioritization during different eras of American history.\textsuperscript{17} Arguably, the first of those objectives (retribution) is unrelated to prevention, while the last three (deterrence, incapacitation, and rehabilitation) all advance the cause of prevention.

In practice, joint efforts to reduce recidivism have contributed to increasing links between the institutions of criminal justice and organizations implementing prevention-based measures to reduce crime. For certain categories of offenders, some level of in-prison rehabilitation programming exists, as does post-incarceration programming for offenders on supervised release. Indeed, as acknowledged in the \textit{United Nations Guidelines for the Prevention of Crime}, preventing recidivism represents one important category of overall crime prevention.\textsuperscript{18} When the criminal justice model is understood as a set of tools formed largely to prevent recidivism, its separation from the social and situational prevention models becomes less absolute. Nonetheless, evaluating other preventive models separately from criminal justice is useful for theoretical clarity.

The other three main crime prevention strands may be summarized in their simplest terms as follows. Developmental prevention operates at the individual level. It entails interventions to prevent the evolution of criminal potential in individuals by targeting evidence-based risk and protective factors.\textsuperscript{19} Community prevention operates more collectively, and entails interventions designed to change the social conditions that influence offending in residential communities or social networks.\textsuperscript{20} Elsewhere in the literature, the broader construct of social crime prevention is used to encompass both developmental and community prevention concepts.\textsuperscript{21} Social crime prevention attempts to influence the factors that make people criminals or cause them to be involved in crime; it can operate on an individual, group, or societal level.\textsuperscript{22} Researchers focus on factors such as societal marginalization, troubled childhoods, and other negative influences, in terms of how those factors contribute to an individual’s eventual engagement in criminal activity.\textsuperscript{23} Finally, based on the premise that much crime is opportunistic, situational prevention endeavors to prevent specific crimes by reducing opportunities to commit them, while increasing the risk and difficulty of doing so.

A contrasting approach to theorizing crime prevention involves importing concepts from the public health literature. This perspective focuses on violence as a threat to community health, rather than primarily as a threat to community order.\textsuperscript{24} From this vantage point, scholars describe primary, secondary, and tertiary levels of prevention.\textsuperscript{25} Primary prevention encompasses efforts directed at entire populations. Secondary prevention is directed at specific risk groups. And tertiary prevention, with the greatest specificity, targets individuals and groups already known to engage in problematic behavior.\textsuperscript{26} When gazing through a public health lens, one may view crimes as “intentional injuries,” which in turn form part of a larger
category of public health problems. This perspective on crime emphasizes prevention over reaction and the reduction of risk factors over the incapacitation of offenders.\textsuperscript{27}

\textit{A New Conceptualization of Crime Prevention}

Existing crime prevention models, as observed by Tore Bjørgo, are generally narrow in scope, do not incorporate key aspects of other models, and "come across as competing prevention models that cannot easily be integrated with each other, either theoretically or as practical strategies for action."\textsuperscript{28} To integrate the strengths of previous approaches into a more holistic model, Bjørgo has put forth a nine-part crime prevention model that incorporates key elements from multiple approaches.\textsuperscript{29} In his book, \textit{Strategies for Preventing Terrorism}, Bjørgo proceeds to apply this general crime prevention model in the terrorism context. Bjørgo’s approach to terrorism prevention is discussed later in this chapter. But in order to reach that point, Bjørgo presents a broad model for crime prevention, and discusses the following critical elements of that model:

1. Establishing and maintaining \textit{normative barriers} to committing criminal acts;
2. Reducing recruitment to criminal social environments and activities by eliminating or reducing the social root causes and individual processes that lead to criminality;
3. Deterrence by getting potential perpetrators to refrain from criminal acts through the threat of punishment;
4. Disruption by stopping criminal acts before they are carried out;
5. Protecting vulnerable targets against criminal acts by reducing opportunities;
6. Reducing the harmful consequences of criminal acts;
7. Reducing the rewards from criminal acts;
8. Incapacitation (or neutralization) by denying perpetrators the ability (capacity) to carry out new criminal acts;
9. Desistance and rehabilitation by making it possible for people who have been involved in, or punished for, crime to return to a normal life.

The steps enumerated above may function as a chain of successive barriers to committing crimes, in which individuals who proceed past one barrier may be stopped by the next one or another following that. For each of the above mechanisms as applied to each type of crime, Bjørgo asserts that we must determine what kinds of measures can be used to activate the mechanisms; who will be the principal actors in charge of implementing the measures; and who are the target groups for the measures. It is also necessary to evaluate the strengths, weaknesses, limitations, and side effects of activating the preventive mechanisms.

In identifying the target groups for various prevention strategies, Bjørgo embraces concepts derived from the public health model. He refers to primary prevention, secondary prevention, and tertiary prevention (as discussed above). Bjørgo also adds a fourth category, which encompasses prevention targeted at victims of crime.\textsuperscript{30} Finally, Bjørgo notes the importance of considering unintended side effects of measures implemented to reduce crime.

Although Bjørgo’s nine-point model and the other models referenced above differ in their orientations and priorities, they jointly shed light on essential parameters of crime prevention. Each one has been elaborated on in significant depth and occupies a substantial place in the literature. The foregoing theoretical sketch, while elementary, provides a bedrock foundation and point of departure for exploring the contributions of the crime prevention literature for the prevention of terrorism.
**Bringing Terrorism Prevention into the Picture: Contributions from Situational Crime Prevention and Other Models**

The prevention of terrorism, as defined in Chapter 2 of this volume, entails the anticipation of risk factors giving rise to terrorist group formation, terrorist campaign initiation, and/or specific attack preparations. In turn, preparedness entails taking proactive and preemptive measures to reduce risks and threats of terrorist crimes and if that turns out to be insufficient, reducing the negative impact of terrorist attacks through a set of planned precautionary measures aimed at strengthening governmental readiness and societal resilience. Along a similarly proactive and preemptive vein, crime prevention refers to efforts to prevent crime or criminal offending in the first instance—before the act has actually been committed.

Terrorism can be described (though not defined) as a particular form of crime—i.e., crime that has a political motive. Therefore, one logical manner of conceptualizing terrorism prevention is as a form of crime prevention. Yet some researchers, policymakers, and other commentators perceive terrorism as fundamentally different from other forms of crime, pointing to a number of terrorism’s characteristics that purportedly distinguish it from “ordinary” crimes. These individuals argue that terrorists’ ideological motivations, and resulting levels of commitment by often fanatical offenders to their causes, render their cost-benefit calculations essentially incomparable to those of ordinary or traditional criminals.

Clarke and Newman have endeavored to refute the perception that terrorism and conventional crime are fundamentally dissimilar. In this pursuit, they consider factors such as the motivations, determination level, funding sources, and scale and organization of events, for both terrorists and conventional criminals. Clarke and Newman conclude that the distinctions between terrorism and conventional crime “rarely stand close scrutiny and from the perspective of situational prevention are of marginal importance.” For present purposes, it is worth simply noting two points. First, acts of terrorism are, in legal terms, crimes and as such, are generally prosecuted by the state and punishable within the criminal justice system. Indeed, many definitions of terrorism incorporate illegality as a necessary element—if the act is not illegal i.e., if it is not a crime, then it is not terrorism. In addition, the conceptual differences between various types of conventional crime—such as murder, rape, or assault on the one hand versus perjury, fraud, or trespassing on the other—arguably are at least as substantive as the supposed differences between crime and terrorism.

Many other researchers, accepting the view of terrorism as a severe form of crime, have increasingly tailored and applied concepts from the crime prevention literature to terrorism prevention in recent years. Within that general framework, many of the resulting studies approach the problem as one of situational crime prevention. Yet other models have been applied in the context of terrorism prevention as well. For example, some have advocated a public health approach, while others have considered routine activities and social learning theories.

It is useful to delve into more detail concerning some of the most relevant crime prevention theories prior to considering their application in the terrorism context. Accordingly, the discussion below begins by addressing situational and environmental crime prevention and their underlying criminological foundations. The discussion will then trace some of the ways in which scholars and practitioners have applied these theories toward terrorism prevention. Finally, this section will address some applications of crime prevention theories other than situational crime prevention in the terrorism context.

**Situational Crime Prevention**

Situational crime prevention (SCP) is essentially “the science of reducing opportunities for crime.” This environmentally-focused approach differs fundamentally from forms of crime
prevention that seek to bring about lasting change in the criminal or delinquent dispositions of individuals. SCP does not focus on dispositions at all, but rather on immediate circumstances as determinants of crime. SCP approaches are thus designed to manipulate environments in ways that make criminal action less attractive by: increasing the difficulties of crime; increasing the immediate risks of getting caught; reducing the rewards of offending; removing excuses for offending; and reducing temptations and provocations.

SCP may be characterized as part of environmental crime prevention, which subsumes both situational approaches and broader planning initiatives. For example, environmental crime prevention may encompass initiatives in urban design and planning. It illuminates temporal and spatial elements that influence offender decision-making, as opposed to social and psychological contributors, and aims to reduce crime by designing or modifying the physical environment to reduce opportunities for crime to occur. SCP thus benefits from the assumption within environmental criminology that contextual factors shape human behavior, including decisions to engage in delinquency and commit crimes. Environmental crime prevention incorporates concepts from place-based approaches including crime pattern theory, routine activities theory, and hot spot analysis, among others.

SCP similarly rests on a foundation or “family” of related criminological theories. These include routine activity theory, crime pattern theory, and rational choice theory. Routine activity theory focuses on the circumstances in which individuals commit predatory criminal acts, rather than focusing on the characteristics of offenders. According to this perspective, the structure of the routine activities of an individual’s life influences criminal opportunities and thereby affects trends in crime. For example, individual routines of traveling to and from work, shopping, or engaging in recreational activities influence the likelihood of when and where a crime will be committed and who will be the victim. According to routine activity theory, the three minimal elements necessary for a crime to occur include a likely offender, a suitable target, and the absence of a capable guardian. Somewhat similarly, crime pattern theory holds that crimes do not occur randomly or uniformly in time, in locations, and in society, but rather result from interactions among a set of sociocultural, legal, economic, and physical variables.

Finally, rational choice theory highlights the process of offender decision-making, and holds that offenders choose to commit crimes for the benefits they confer. Criminals are understood to thoughtfully weigh the costs and benefits of alternative courses of conduct prior to their target selection and planning. In applying this model to specific crimes, it is helpful to evaluate the choice structuring properties that factor into offender decisions. Choice structuring properties include the characteristics of offenses “such as type and amount of pay-off, perceived risk, skill needed and so on” that the offender perceives as “especially salient to his or her goals, motives, experiences, abilities, expertise, and preferences.” Understanding and anticipating these decision-making processes enables the prevention of crime. Together with routine activity theory and crime pattern theory, rational choice theory contributes some of the related foundational tenets underlying SCP.

Applications to Terrorism Prevention and Preparedness

In recent decades, researchers have applied SCP principles to the prevention of terrorism. Clarke and Newman initiated this trend with the publication of their pioneering book, *Outsmarting the Terrorists*, in 2006. Therein, the authors assert that terrorism is a form of crime in all essential respects, albeit crime with a political motive. They set out to view terrorism through the lens of opportunity reduction. The authors argue that by using SCP techniques to remove opportunities for terrorism to occur, societies can reduce the incidence of attacks. However, new opportunities must be continuously re-evaluated as terrorists adapt to their changing environments. Following publication of *Outsmarting the Terrorists*, researchers have increasingly focused on applying criminological perspectives to terrorism,
often through the lens of SCP. While some scholars consider how to change the dispositions of terrorists by exploring “the applicability of traditional sociological theories of crime to terrorism,” others follow Clarke and Newman’s example by focusing instead on removing opportunities for terrorist crimes. This latter group resolved to “eschew the intractability of individual behavior and note the promise of preventing terrorist crimes by altering their environments.”

The Early Intersection of Situational Crime Prevention with Terrorism Prevention

Analyzing the opportunity structure for terrorism, as described by Clarke and Newman, involves considering the arrangements of everyday life that create opportunities ripe for exploitation by terrorists. Thus, the authors apply the underlying principles of routine activity theory, crime pattern theory, and rational choice theory – all integrated within a SCP approach – to the politically motivated crime of terrorism.

Beginning with the assumption that “all human action is the outcome of an interaction between motivation and opportunity” – also described as the interaction between organism and environment – Clarke and Newman focus on the latter component of this equation by analyzing the opportunity structure for terrorism. To shed light on the concept of terrorist opportunity, they divide such opportunity into four pillars, comprising targets, weapons, tools, and facilitating conditions. The authors additionally distill twenty principles from the crime prevention literature that, taken together, help construct an approach for “outsmarting the terrorists.” Collectively, these twenty principles require experts to “identify the opportunity structure of particular kinds of terrorist attacks, describe the steps that terrorists take from the beginning to the end and aftermath of their terrorist attacks and finally, identify points at which we may intervene in order to interrupt the terrorist’s journey to destruction.”

To undertake this comprehensive type of SCP analysis, one must “think [like a] terrorist.” For example, one can attempt to replicate the decision-making process of terrorists in considering the first pillar of terrorist opportunity, which involves the selection of targets. Assessing the relative attractiveness and vulnerability of potential targets in the same manner as a terrorist might do facilitates the establishment of priorities for protection in terms of target hardening. For addressing single-terror attacks undertaken by foreign-based terrorists (e.g., the 9/11 attacks), the authors propose an EVIL DONE analytical framework. This acronym indicates that targets considered attractive by terrorists are those which encompass some combination of the following characteristics: Exposed, Vital, Iconic, Legitimate, Destructible, Occupied, Near, and Easy.

After identifying terrorists’ preferred targets, the individuals and organizations charged with outsmarting them – i.e., governments, businesses, and security professionals – should take steps to interfere with terrorists’ abilities to attack those targets at greatest risk. For this purpose, they may impose target hardening measures, or devise ways to reduce the perceived rewards for certain types of attacks. Accordingly, the EVIL DONE framework is designed to facilitate more efficient resource allocation than if all targets in society were considered equally vulnerable and in need of equal levels of protection. Implicitly, the benefits obtained by hardening targets in this manner are contingent upon the strength of the EVIL DONE template as an assessment tool. Other researchers have studied the EVIL DONE template and endeavored to extend Clarke and Newman’s work on terrorists’ target selection further, as discussed in the next section.

Clarke and Newman propose a similar analysis to EVIL DONE for understanding and assessing terrorists’ choices of weapons, for which they use the acronym MURDEROUS. This framework incorporates nine attributes thought to guide terrorist actors’ choices of weapons, including Multipurpose, Undetectable, Removable, Destructive, Enjoyable, Reliable, Obtainable, Uncomplicated, and Safe. The implication is that by understanding which weapons
are most attractive to terrorists and why, authorities will be better positioned to interfere with terrorists’ opportunities to obtain those weapons and their perceived rewards for doing so. Roughly speaking, terrorists’ weapons may be grouped into the following three categories: guns and other small arms; explosives; and unconventional weapons, including nuclear-related, chemical, and biological weapons (sometimes referred to as weapons of mass destruction or WMDs). Application of the MURDEROUS template can help illuminate how terrorists make choices within and among these three classes of weapons.

Finally, Clarke and Newman afford consideration to tools and facilitating conditions, the remaining two pillars of terrorist opportunity, and the “major factors that bring weapons and targets together.” While tools are tangible products such as cars, trucks, credit cards, false identification documents and cell phones, facilitating conditions are social and physical arrangements of society that make it easier for terrorists to perpetrate attacks. Three main approaches for tightening controls on tools include: modifying the tools themselves to make them more difficult for terrorists to use; tightening up their supply or reducing their accessibility to terrorists; and tracking their distribution to determine who has acquired them. The authors conclude that efforts to reduce terrorism have not sufficiently addressed tools as such, and that “much more could be done to make life difficult for the terrorists by developing controls on the many products that they routinely use.”

Regarding facilitating conditions, Clarke and Newman identify five categories—those that make crime Easy, Safe, Excusable, Enticing, and Rewarding (ESEER). The authors argue that analysis of these conditions, much like analysis of the other pillars of terrorist opportunity, can help to identify preventive options. First, one must recognize that facilitating conditions are of varying importance, and not all of them are susceptible to change. Therefore, after identifying relevant facilitating conditions to a given type of terrorism, one should assess the chances of successfully mitigating those conditions, as well as the potential benefits of doing so. In assessing the potential benefits, one should consider whether the condition facilitates not just the targeted form of terrorism, but other forms as well. For example, Clarke and Newman, writing in 2006, note that certain lax conditions at the border may facilitate terrorists’ opportunities to smuggle plutonium or uranium into the US for the assembly of a nuclear bomb; but in analyzing the relevant border conditions, one should note that the conditions also facilitate the unlawful entry of other weapons of terrorism and even of terrorists as well. By mitigating facilitating conditions, societal actors can increase the risks and difficulty of the targeted form of attack, while reducing its rewards and eliminating excuses and enticements.

An important consideration related to SCP approaches and the environmental changes they produce relates to considering the costs these approaches impose on privacy and civil liberties. Clarke and Newman argue that SCP compares favorably to intelligence-led approaches to counterterrorism, such as those that may be relied upon to “take out” terrorists. Intelligence-led policing “necessitates the collection of enormous amounts of information without any way to assess its relevance in predicting which individuals may commit the next terrorist attack.” In contrast, when using SCP approaches, there are many instances in which one can insert broad obstacles to terrorist planning and action without needing to know the identities or other personal information about the potential terrorists at all. The emphasis in SCP is not on predicting a particular attack by any specific individual, but rather on anticipating different kinds of attacks and, accordingly, designing and implementing measures that interfere with terrorists’ opportunities to commit those kinds of attacks.

An implicit premise when addressing terrorism as crime rather than as a national security threat is that not all terrorist attacks will be stopped, but their likelihood will be reduced. As Alex Schmid has noted, SCP approaches therefore may help to “de-escalate unrealistic expectations” about eradicating the terrorist threat entirely. Similarly, emphasizing SCP can help put the terrorism threat in perspective because, “[l]ike many other forms of crime,
terrorism will probably never go away – but it can be made a manageable risk if there is greater focus on situational and structural prevention.”

Despite clear differences, SCP and other criminological perspectives are not mutually exclusive. Rather, environmental and situational approaches, including SCP, may complement perspectives that focus on psychological and social causes of terrorism – sometimes also referred to as “root causes.” Accordingly, counterterrorism professionals may pursue different strands of crime prevention simultaneously. Militarized approaches to terrorism prevention – notably, efforts to eliminate or incapacitate known terrorists – may also be pursued simultaneously with crime prevention approaches. However, SCP proponents generally advocate against allowing efforts to “take out” terrorists dominate society’s response to terrorism. Rather, SCP in the terrorism context incorporates the assumption “that there will usually be an unlimited supply of potential terrorists who adhere to aggrieved ideological movements and whose goals are difficult to satisfy”. In addition, SCP proponents argue from a practical standpoint that efforts to eradicate terrorists are simply unlikely to work, just as imposing severe punishments on conventional criminals has not deterred and stopped crime.

In Outsmarting the Terrorists, Clarke and Newman lay the foundation for a new approach to terrorism prevention based on SCP. This approach emphasizes that terrorists confront circumstantial and logistical challenges just as other criminals do, and that societies can diminish the incidence of terrorism by studying and reducing the opportunities to commit terrorist acts. Meaningful analysis of terrorist opportunities is facilitated by breaking such opportunities into their fundamental components – targets, weapons, tools, and facilitating conditions – and then using the concepts introduced by Clarke and Newman to understand, anticipate, and take steps to manipulate terrorist decision-making. However, these foundations, as described by Clarke and Newman, are largely conceptual.

In the intervening years since publication of Outsmarting the Terrorists, a few researchers have tested the concepts advanced therein, but most subsequent studies applying SCP to terrorism have not endeavored to empirically assess Clarke and Newman’s claims. Nonetheless, substantial progress has been made in extending the principles underlying Clarke and Newman’s work and applying crime prevention approaches in a wide array of terrorism contexts.

**Subsequent Applications: 2006-2019**

Researchers have continued to apply SCP and other crime prevention principles to terrorism prevention in the wake of Outsmarting the Terrorists (2006). In this section, subsequent studies pertaining to SCP are discussed, a few examples are highlighted, and significant absences are identified. Freilich, Gruenewald, and Mandala add clarity to the developing intersection of SCP and terrorism in 2019, when they published an overview entitled Situational Crime Prevention and Terrorism: An Assessment of 10 Years of Research. That article systematically reviews the literature between 2006 and 2016, as it concerns SCP’s intersection with terrorism prevention. The table below, reproduced from the article by Freilich et al., indicates the number of relevant publications each year during the designated period. In total, Freilich and colleagues identify 60 such studies. Relevant publications peaked in 2009 with 11 in total that year. This increase was attributable to a special issue of Crime Prevention Studies in 2009, focusing exclusively on the application of SCP principles to terrorism and including contributions from several prominent authors.

In their review, Freilich and colleagues analyze selected attributes of the 60 identified publications in order to present an overview of scholarship at the nexus of SCP with terrorism. For each publication, they examine variables related to the professional backgrounds of authors; publication outlets; methods used; and countries and terrorist groups that were the subjects of the studies. Although the studies all relate in some manner to the application of SCP to terrorism, their topics extend to far-ranging subject matters, largely reflecting the broad
diversity of acts and events covered under the rubric of terrorism itself. For example, chapters from the special issue of Crime Prevention Studies cover areas as diverse as the spatio-temporal modeling of insurgency in Iraq, bioterrorism, and hostage-taking and kidnapping with a case study of Korean hostages in Afghanistan, among several others.

### Table 1. Year of Publication

<table>
<thead>
<tr>
<th>Year</th>
<th>Frequency</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>1</td>
<td>1.7</td>
</tr>
<tr>
<td>2007</td>
<td>4</td>
<td>6.7</td>
</tr>
<tr>
<td>2008</td>
<td>3</td>
<td>5.0</td>
</tr>
<tr>
<td>2009</td>
<td>11</td>
<td>18.3</td>
</tr>
<tr>
<td>2010</td>
<td>3</td>
<td>5.0</td>
</tr>
<tr>
<td>2011</td>
<td>6</td>
<td>10.0</td>
</tr>
<tr>
<td>2012</td>
<td>10</td>
<td>16.7</td>
</tr>
<tr>
<td>2013</td>
<td>6</td>
<td>10.0</td>
</tr>
<tr>
<td>2014</td>
<td>3</td>
<td>5.0</td>
</tr>
<tr>
<td>2015</td>
<td>9</td>
<td>15.0</td>
</tr>
<tr>
<td>2016</td>
<td>4</td>
<td>6.7</td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td>100</td>
</tr>
</tbody>
</table>

Despite increasing interest in the intersection of SCP with terrorism, Freilich and colleagues observe that academics have “generally failed to respond” to the arguments made in Outsmarting the Terrorists by subjecting Clarke and Newman’s claims to scientific verification. To wit, only five of the 60 studies identified by Freilich and colleagues empirically test concepts derived from Clarke and Newman’s EVIL DONE framework for assessing the attractiveness of targets. Only one of the 60 studies empirically tests MURDEROUS, the template Clarke and Newman proposed for assessing terrorists’ choice of weapons. And none of the 60 studies endeavored to empirically examine Clarke and Newman’s claims concerning terrorists’ tools, nor the ESEER framework for facilitating conditions.

While it is not possible to discuss each study that applies SCP principles in a terrorism-related context, it is worth briefly considering a few examples here to illustrate how subsequent works have begun to test and flesh out critical concepts. The examples that follow are limited to the context of terrorist target selection, with a focus on Clarke and Newman’s EVIL DONE framework. As discussed above, Clarke and Newman describe a theory according to which terrorists’ selection of targets is largely based on tactical considerations. Capturing this view, the EVIL DONE acronym indicates features that terrorists are presumed to most value in their targets. Those targets most aligned with the EVIL DONE framework are considered most attractive and vulnerable. Specifically, targets are ostensibly more attractive and vulnerable to terrorists when they are Exposed, Vital, Iconic, Legitimate, Destructible, Occupied, Near, and Easy.

Subsequent studies have further illuminated the dynamics of terrorist target selection. Rachel Boba’s chapter in the special edition of Crime Prevention Studies endeavors to refine the EVIL DONE framework by further deconstructing each of its eight components into a set of items that can be scored easily and measured consistently across targets. Boba provides a risk assessment methodology for local officials and researchers to evaluate the likelihood of terrorist attacks for individual targets, and strategies for aggregate analysis of groups of targets within local jurisdictions. The purpose of these methodologies is to enable officials to prioritize individual targets and groups of targets according to their respective needs for protection. Boba sets forth a scoring system for evaluating the EVIL DONE factors in more detail than previously existed in the literature, bringing the field “another step closer to quantifying and standardizing assessment of vulnerability based on the EVIL DONE approach.” Thus, while
Boba does not actually test the EVIL DONE framework nor apply it to potential targets, she extends the original template as set forth by Clarke and Newman to render it more readily usable by local officials and researchers.

More recently, in 2015, researchers analyzed the EVIL DONE target selection principles in connection with eco-terrorism, seeking to descriptively assess the attractiveness and vulnerability of targets selected by environmental and animal rights extremists. The authors note that previous applications of SCP to terrorism were largely concentrated in the area of Islamist extremism, and posited (referencing Clarke and Newman) that the target selection process is likely to vary among forms of terrorism rooted in different backgrounds and ideologies. Accordingly, the authors venture away from Islamist ideologies and instead selected the relatively unexplored arena of target selection among eco-terrorists.

While Boba’s work focuses on providing a risk assessment methodology and strategies, Gruenewald and colleagues take the next step by actually applying the EVIL DONE model to targets that had previously been attacked. Their goal is to empirically examine how key characteristics of actual targets influenced the decision-making of eco-terrorists in the United States. Using the eight attributes of EVIL DONE for measurement, the study’s authors evaluate the extent to which eco-terrorists select targets based on vulnerability and attractiveness. Eco-terrorism is defined to include ideologically motivated crimes committed by environmental and animal rights extremists, occurring between 1987 and 2012. Data were extracted from the American Terrorism Study (ATS), a database which monitors federal prosecutions of accused terrorist offenders and is housed at the University of Arkansas. In turn, the ATS relies on the definition of eco-terrorism provided by the Federal Bureau of Investigation (FBI): “the use or threatened use of violence of a criminal nature against innocent victims or property by an environmentally oriented, subnational group for environmental-political reason, or aimed at an audience beyond the target, often of a symbolic nature.” Based on their findings about the relative importance of different EVIL DONE attributes in rendering targets attractive and vulnerable, the authors provided preliminary policy recommendations for reducing the vulnerability of potential targets to eco-terrorism incidents.

While researchers have explored the application of SCP principles to terrorism, practitioners and policymakers have in turn utilized those principles for practical terrorism prevention. Some governments have effectively implemented SCP strategies to protect their public spaces. For example, in the United States, the Department of Justice published a guide, Policing Terrorism: An Executive’s Guide, in which Newman and Clarke provide guidance for police chiefs and other senior executives to utilize methods often reflecting SCP principles. In Britain, the Protect strand of the government’s CONTEST strategy for counterterrorism essentially entails the application of SCP principles and target-hardening approaches. The National Counter Terrorism Security Office, a police unit that supports the Protect and Prepare strands of CONTEST, has recommended crime prevention measures to inhibit opportunities for committing terrorist acts. The office’s advice booklet for businesses provides guidelines including recommendations for good lighting, closed circuit television (CCTV), perimeter fencing, and removal of exterior planting that obscures surveillance as protective measures, “as the presence of situational factors providing guardianship increases the risk of apprehension.” The development of a protective “ring of steel” consisting of CCTV cameras, linked to real time computer-based analytics around significant locations in London’s financial district has also been cited as an example of the implementation of SCP principles to prevent terrorism. Other countries have implemented similar approaches to protect financial districts and other urban spaces as well.

Yet some researchers highlight the need for caution in looking to SCP strategies to protect public spaces from terrorism. Fussey contends that while target-hardening strategies clearly hold a place in countering terrorism, awareness of the “caveats and limitations” of these strategies “facilitates a more nuanced, appropriate and effective application.” A study by
Robinson, Marchment and Gill examines whether domestic extremist crimes causing property damage were similar to property damage incidents perpetrated by conventional criminals. The results suggest that left-wing extremists do not behave in the same manner as conventional criminals, in that the left-wing extremists studied were “less likely to conform to theoretical expectations regarding the effect of guardianship on target selection decisions.” Specifically, the presence of lighting and CCTV at a target location is found to be less of a deterrent for those engaged in domestic extremist activity (in the form of direct action attacks) than for those engaged in conventional crime. Thus, while the SCP approach to terrorism prevention has gained traction, it may be more effective in relation to some threat areas than others. Continuing research will help to clarify the best applications for SCP in terrorism prevention, and perhaps shed light on the optimal manner of combining these strategies with other crime prevention and counterterrorism strategies to form a more holistic paradigm.

Benefits, Drawbacks, and Future Directions

In considering the optimal method of combining SCP with other crime prevention approaches – and combining the criminological perspective with those of other disciplines – it is useful to have a sense of the strengths and limitations of SCP in this domain.

One strength of the SCP approach is its pragmatism, reflected in its assumption that there is no possibility of “taking out” all terrorists. Rather, groups will replenish themselves and individuals who leave or are “eliminated” will be replaced by new recruits. Accordingly, SCP eschews the idea of attempting in vain to eradicate every terrorist and focuses more fruitfully on the attainable goal of reducing terrorist opportunities. Similarly, SCP does not endeavor to identify or address the biological or social factors that cause individuals to radicalize, but simply seeks to reduce opportunities across the board for terrorist acts to occur. Thus, to the extent it prevents terrorism, SCP is likely to do so in more immediate and tangible ways than approaches emphasizing criminal “dispositions.” Further, addressing terrorism through the lens of situational crime prevention may lower societal and cultural expectations for its complete eradication, and contribute to a more balanced perception of terrorism in relation to other threats. Finally, SCP may result in a “diffusion of benefits,” which refers to reductions in crime or terrorism that extend even further than the crimes targeted by preventive measures introduced.

Yet, critics raise important points concerning the limitations and drawbacks of approaching terrorism through an SCP framework. First, some criminologists and others argue that by neglecting the need to explain why people commit crimes of terrorism, SCP incorporates an insurmountable flaw. In this view, by focusing on reducing opportunities through environmental change rather than criminal dispositions, SCP presents an “overly simplistic” approach, while “ignoring the myriad of sociological, psychological, political, and other explanatory factors.” Another way of expressing this type of criticism is to say that SCP treats the “symptoms” of terrorism rather than the causes. Essentially, it may provide a band-aid solution, but neglects to address the persistent “root causes” that push and pull individuals to commit terrorist crimes. Similarly, SCP may be flawed in that it applies a “one-size-fits-all” model, rather than properly accounting for terrorists’ actual motivations and perspectives.

Another perceived drawback of SCP relates to the idea of displacement, though the extent to which this phenomenon occurs is contested. The argument for displacement holds that if an individual is prevented from completing a contemplated or aspirational terrorist act through SCP measures, the individual will simply redirect his or her nefarious efforts to another, softer target. The higher commitment levels presumed to motivate acts of terrorism are seen as support that would-be perpetrators will not be deterred. For example, the trend among perpetrators of international terrorism to target large numbers of defenseless civilians may be perceived as a response to the “hardening” of more symbolic targets through the addition of
new layers of security. Yet Clarke and Newman, among others, argue that the risk of displacement has been overstated. Indeed, Freilich, Gruenewald, and Mandala assert that “[b]ecause different types of terrorism have varying opportunity structures, successful intervention against one form of terrorism attack will usually not result in displacement to another.”

One example often cited in support of the argument against displacement relates to the success authorities achieved at reducing aircraft hijackings—without any clear redirection to aircraft bombings—through added security measures following the wave of hijackings in the late 1960s and early 1970s.

Researchers sometimes draw a distinction between displacement and adaptation, with displacement perceived as an immediate shift in plans and adaptation occurring along a longer time horizon. Criminal adaptation is the process in which offenders circumvent preventive measures over time. Thus, while Clarke and Newman do not perceive displacement as a realistic drawback to their SCP approach, they nonetheless acknowledge the idea that terrorists will react to changes in their environments and opportunities by attempting to exploit new opportunity structures that present themselves. Accordingly, security professionals should anticipate the new approaches terrorists are likely to take.

SCP may also provide a more realistic strategy in some locations and geopolitical climates than others. Generally, SCP approaches are more suited than military ones to deal with forms of terrorism that appear in stable societies. On the other hand, the approach is less applicable when terrorism develops into guerrilla warfare, or is part of an insurgency, as in Afghanistan, Syria, and Iraq.

One challenge to researching the merits and effectiveness of SCP is the difficulties academics encounter in accessing official, crime-related data to study terrorism in the US and many other countries. Freilich and colleagues suggest that SCP researchers should “think creatively about strategies to gain the cooperation of official agencies to [gain] access to their terrorism data.” Increased access to official data, rather than having to rely exclusively on open source data, could help scholars to devise more effective terrorism prevention strategies in the criminological realm.

Additionally, Freilich and colleagues highlight the dearth of empirical testing to validate the claims and arguments advanced by Clarke and Newman in *Outsmarting the Terrorists*. In particular, the counterterrorism community stands to benefit from empirical evaluations of Clarke and Newman’s four pillars of terrorist opportunity. In connection with target selection, preliminary studies of the EVIL DONE framework shed light on how this type of research can be helpful from a pragmatic and policy standpoint. In the study of EVIL DONE’s application with respect to target selection for eco-terrorism crimes, Gruenewald and colleagues interestingly observed that some of the eight EVIL DONE measures are likely interrelated, and therefore may reflect overlapping dimensions of target vulnerability and attractiveness. The authors suggest that future research would be well advised to utilize data reduction techniques and multivariate analyses “to identify… conceptually distinct measures of key target attributes.” In addition, the authors note that a better understanding of target vulnerability and attractiveness may emerge by comparatively studying the relative risks to targets across various terrorist movements (beyond eco-terrorism), such as right-wing terrorism and international terrorism. Similarly, future studies could empirically evaluate Clarke and Newman’s ESEER template for facilitating conditions. Freilich and colleagues point out that accounting for ideology in target selection could help to enhance the usefulness of the EVIL DONE template. Studies along the foregoing dimensions require sophisticated methods and a rigorous design.
Beyond Situational Crime Prevention: The Broader Nexus of Criminology, Crime Prevention, and Terrorism

Scholars have increasingly sought to explore the ways in which criminology and terrorism studies may each benefit from developments on the other side of the disciplinary fence, including but also extending beyond the use of SCP and closely related approaches such as routine activities and rational choice. Some researchers have begun studying the application of other foundational models in criminology, such as strain theory\(^{117}\) and social disorganization theory,\(^{118}\) in terrorism-related contexts. Finally, Tore Bjørgo has developed a broad crime prevention approach that incorporates both SCP principles and other preventive strategies, and has demonstrated how that approach can provide a more comprehensive response than previous strategies to the wide-ranging terrorist threat.

There are many ways in which criminological theories might be applied to the study of terrorism, and researchers have only begun to scratch the surface. In comparison to SCP, however, some other areas of study within criminology are more variable in terms of the directness of their relationship with terrorism prevention. A special issue of the journal *Terrorism and Political Violence*, published in 2015, was devoted entirely to criminological approaches to the study of terrorism. In their introduction to that special issue, Freilich and LaFree note that prior criminological studies of terrorism generally employed the perspectives of crime prevention models such as routine activities theory, rational choice theory, and SCP, and that further expansion into other major criminology frameworks would be beneficial. The authors reference social learning, classic strain, social control, life course, and psychological and biological perspectives as other models into which terrorism-related research could beneficially expand.\(^{119}\) The special issue itself constitutes a “step in this direction,” with articles addressing anomie/strain, social disorganization, and under-explored routine activities frameworks.\(^{120}\)

In two related examples of research using criminological theories, Gary LaFree published articles respectively with Bianca Bersani in 2014,\(^{121}\) and Susan Fahey in 2015,\(^{122}\) exploring social disorganization theory in relation to terrorist attacks at the county level within the US, as well as at the country level. The implications of this work highlight the significance of place to finding patterns in the occurrence of terrorist violence. Drawing from the work of French sociologist Emile Durkheim on “anomie,” social disorganization may be conceptualized as the “inability of individuals within communities to self-regulate or to realize shared values and solve commonly experienced problems,” something thought to result from rapid social change.\(^{123}\) A socially disorganized area “is one in which the residents are unable to prevent crime and deviance due to their inability to realize widely shared norms.”\(^{124}\)

Fahey and LaFree explore the connection between state instability and the incidence of terrorist attacks, focusing on ethnic war, revolutionary war, adverse regime change, and genocide as sources of instability. They found that politically unstable countries consistently experienced high levels of terrorist attacks and resulting fatalities. In considering the geographical concentration of terrorist attacks at the county level within the US, LaFree and Bersani found that terrorist attacks were more common in countries characterized by greater population heterogeneity and more residential instability. However, the findings are contrary to social disorganization theory predictions relating to concentrated disadvantage and its impact. In other words, some measures from social disorganization theory are useful for predicting geographical locations more at risk of terrorist attacks, while other measures are not. Further research along these lines could have important policy implications for the allocation of international and national resources to terrorism prevention.

An alternative approach to preventing terrorism derives from public health models. The roots of the public health approach are intertwined with criminology. Over twenty years ago, Moore wrote that the costs associated with violent crime constitute “an expensive part of the [United States’] overall health bill.”\(^{125}\) As applied to terrorism in the wake of the 9/11 attacks,
this argument is particularly compelling. The US House of Representatives recently passed legislation to extend funding for the September 11th Victim Compensation Fund through 2090, covering the lifetime health expenses of first responders to the 9/11 attacks. The estimated cost of fully funding the trust is US $10.2 billion, in addition to the previous funding of nearly US $7.4 billion. Recent research has focused on the ways in which public health research and practice can inform the prevention of violent extremism or "violent radicalization." Bhui and colleagues argue that, in efforts to prevent terrorism, “epidemiology, psychology, sociology and other behavioral sciences can contribute important data towards prevention strategies, which have been used in public health programs to address violence.” Public health approaches may be perceived as complementary to criminal justice, and may be contextualized within a broader framework of “countering violent extremism.”

Conclusion

Viewing terrorism fundamentally as crime – and informing policy from a perspective rooted in criminology and crime prevention – represents a shift from traditional approaches to terrorism studies, which more frequently draw from psychology and political science. While researchers and practitioners highlight both pros and cons of linking the prevention of terrorism with that of conventional crime, including organized crime, it is generally acknowledged that criminology holds at least some degree of value for the prevention of terrorism. However, much of that value remains currently untapped and under-explored. Nevertheless, the interdisciplinary nexus of terrorism studies and criminology has been gaining momentum over recent decades.

SCP models have been considered for terrorism prevention purposes with relative frequency as compared with other criminological models. SCP offers pragmatic strategies for reducing the occurrence of terrorism by diminishing opportunities for it to occur. This approach excludes consideration of the reasons why terrorists perpetrate their crimes, and strives only to block their opportunities and reduce their perceived rewards for doing so. In less immediate but still crucially important ways, other models of crime prevention provide valuable strategies as well. Tore Bjørgo’s nine-point crime prevention model recognizes this, and therefore incorporates, but also extends beyond SCP principles.

A review of the developing literature suggests that practitioners, policymakers, and researchers seeking to advance terrorism prevention and preparedness would be well-advised to tailor and incorporate crime prevention approaches into their work. Many criticisms of applying a crime prevention approach to the prevention of terrorism may be addressed through the recognition that approaches rooted in criminology need not be implemented to the exclusion of other methods, and are undoubtedly enhanced through interdisciplinary perspectives. As part of a holistic approach extending across disciplines, additional work grounded in criminology and crime prevention applications stands to offer substantial benefits for the field of terrorism prevention and preparedness.

Kelly A. Berkell is an Attorney and a Senior Research Fellow at the Center on Terrorism at John Jay College of Criminal Justice, City University of New York. She previously served as the National Security Fellow at Fordham Law School’s Center on National Security, focusing on terrorism and cybersecurity. A graduate of New York University School of Law and Barnard College, As Attorney, Kelly Berkell previously practiced securities and white-collar criminal litigation, and served as Legislative Counsel to a New York State Assembly Member. Her current research focuses on preventing and countering violent extremism, particularly where initiatives intersect with United States laws and the criminal justice system. Her writing on these topics has appeared in the “Harvard National Security Journal” and the “Journal for Deradicalization.”
Endnotes

9 Welsh and Farrington 2012, p. 128.
10 Gruenewald et al. 2015.
12 For example, see Freilich and LaFree 2015, p. 6.
14 Tonry and Farrington 1995.
15 Bjørgo 2013, p. 9.

19 Welsh and Farrington 2012, p. 128.

20 Crawford and Evans 2017. In some contexts, community safety has been suggested as either overlapping generally with community prevention, or as an umbrella term to substitute for “crime prevention.”


22 Bjørgo 2013, p. 9.

23 Ibid.


26 Bjørgo 2013.

27 Moore 1995. Tonry and Farrington reject an overtly public health-focused typology, arguing that the approach may be less useful, as “only specialists are likely to understand the distinctions being made.” Tonry and Farrington 1995, p. 2. Yet they clarify that developmental, community, and situational prevention all contain elements of the public health approach. Others, such as Bjørgo, incorporate concepts relating to primary, secondary, and tertiary prevention into models containing elements from the other major approaches as well, as discussed below.

28 Bjørgo 2013, Preface.

29 Bjørgo also discusses the risk management model of crime prevention. This approach involves tailoring prevention efforts in proportion to the threat levels presented by particular crimes. Threat levels, in turn, are measured as the product of the would-be perpetrator’s intention, and ability to effectuate that intention. Similarly, the risk of the specified crime is measured as the product of the probability of its occurrence and the magnitude of the consequences, should the event occur. In this model, risk can be diminished by reducing intention, capacity, vulnerability, or consequences. Bjørgo 2013, p. 10.


31 Welsh and Farrington 2012, p. 128.

32 Gruenewald et al. 2015, p. 436.


34 Ibid. 2006, p. 6.


36 E.g., Bhui, Kamaldeep, et al., ‘A Public Health Approach to Understanding and Preventing Violent Radicalization,’ BMC Medicine, 10(1), 2012, p. 16.


40 Clarke 2018.
Freilich et al. 2019. The relationships of different criminological theories in this arena to one another is described in varying ways in the literature. For example, environmental criminology has been described at times as essentially synonymous with crime pattern theory (e.g., Gruenewald et al. 2015), or, alternatively, as resting upon it. Regardless of the precise configuration of the relationships between these theories, they clearly comprise related theories forming a mutually reinforcing branch of criminology.

45 Gruenewald et al. 2015.


51 Brantingham and Brantingham, 1993.

52 Clarke and Harris 1992, p. 25.

53 Gruenewald et al. 2015.

54 Cornish and Clarke 1987, p. 935.

55 Gruenewald et al. 2015.


57 Ibid.


59 Ibid., p. 32.


61 Clarke and Newman 2006, p. 7. The 20 principles that Clarke and Newman interpret from the SCP literature for outsmarting the terrorists are: 1) We must not rely on changing the hearts and minds of terrorists (i.e., we should focus on reducing terrorists’ opportunities rather than exclusively on reducing their motivations); 2) we must not depend on “taking out” the terrorists; 3) we must develop solutions for each distinct form of terrorism; 4) we must accept that terrorists are rational (i.e., incorporating rational choice theory); 5) we must learn how terrorists accomplish their tasks; 6) we must control the tools and weapons of terrorism; 7) we must concentrate preventive resources on the most vulnerable targets; 8) we must formulate separate preventive policies for terrorism at home and overseas; 9) we must accept that the threat of terrorism will never disappear; 10) we must always be one step ahead; 11) we must learn from the past and anticipate the future; 12) we must match the rationality of terrorists in devising solutions; 13) we must beware of the magic bullet; 14) we must make security decisions within the context of predetermined budgets; 15) we must ensure that
federal antiterrorism budgets are disbursed according to risk; 16) we must not depend on government to do it all; 17) we must develop dual benefit solutions; 18) we must not take public good will for granted; 19) we must not let secrecy be a cloak for incompetence; and 20) we must not be daunted by the enormous task before us.  

62 The analogue in the crime prevention literature, which serves as the basis for Clarke and Newman’s terminology, is to “think thief.” Clarke and Newman 2006, p. 20.  

63 Ibid. p. 15.  

64 Ibid., p. 117.  

65 Ibid., p. 121.  

66 Ibid., p. 125.  

67 Ibid., p. 134.  

68 Ibid., p. 204.  

69 Ibid.  

70 Ibid. p. 207.  


72 Bjørgo 2013.  


75 Newman and Clarke 2008.  


77 Ibid.  

78 Ibid., pp. 1292-1293.  


82 Freilich et al. 2019, p. 1296.  

83 Ibid., p. 1300. Subsequent to the time period examined by Freilich and colleagues, however, two of the study’s authors tested the MURDEROUS framework in a separate study comparing successful and unsuccessful terrorist assassinations. Consistent with the MURDEROUS framework, they found that assassinations were more likely to succeed when terrorists use firearms rather than explosives. Mandala, Marissa and Joshua D. Freilich, ‘Disrupting Terrorist Assassinations Through Situational Crime Prevention,’ Crime and Delinquency, 64(12), 2018, pp. 1515-1537.  


85 Freilich et al. 2019, p. 1296.  

86 This target selection framework has received more attention than other concepts relating to terrorist opportunity discussed in Ronald and Newman 2006.  


88 Ibid, p. 77. A doctoral dissertation by Stacy Paton also explored EVIL DONE as a vulnerability assessment. Primary goals of the thesis were to present the EVIL DONE

89 Gruenewald et al. 2015.
91 Fussey 2011, pp. 86, 88.
93 Fussey 2011. However, the “ring of steel” around London’s financial district was set up already in the 1990s.
95 Ibid, p. 88.
97 Schmid 2012.
99 Gruenewald et al. 2015, p. 449.
101 Ibid.
102 Fussey 2011, p. 95.
103 Bjørgo 2013, pp. 67-68.
104 Clarke and Newman 2006, p. 27.
105 Freilich et al. 2019, p. 1287.
110 Ibid.
112 Ibid.
113 Ibid, p. 1296.

119 Freilich and LaFree 2015, p. 2.

120 Ibid.

121 LaFree, Gary and Bianca E. Bersani, ‘County-Level Correlates of Terrorist Attacks in the United States,’ *Criminology and Public Policy*, 13(3), 2014, pp. 455-481.

122 Fahey and LaFree 2015.


124 Fahey and LaFree 2015, p. 82.


128 Bhui et al. 2012.

129 Ibid., p. 2.

130 Ibid; Moore 1995.

Bibliography


LaFree, Gary and Bianca E. Bersani, ‘County-Level Correlates of Terrorist Attacks in the United States’, Criminology and Public Policy, 13(3), 2014, pp. 455-481.


Robinson, Arlene, Zoe Marchment, Paul Gill, ‘Domestic Extremist Criminal Damage Events:..
Web-based Resources

Australian Institute of Criminology, ‘Crime Prevention Approaches, Theory and Mechanisms.’

National Institute of Justice, ‘Community Crime Prevention Strategies.’

https://www.crimesolutions.gov/PracticeDetails.aspx?ID=42.


Chapter 4
De-Exceptionalizing the Terrorist Phenomenon: Lessons and Concepts from Conflict Prevention and Transformation
Andreas Schädel and Hans J. Giessmann

This chapter shows how approaches, concepts, and instruments from conflict prevention and conflict resolution practice can be of use in conflicts marked by terrorist violence. Based on the assumption that terrorism and its effective prevention can only be understood as part of a wider political conflict and in combination with the surrounding structural power relationships, we examine how the instruments of negotiations and dialogue, although still categorically refused by some terrorism scholars and policymakers, can prove valuable additions to existing approaches of terrorism prevention.

The chapter begins with a conceptual critique of classical realist definitions of terrorism and shows how their homogenization and trivialization of the phenomenon helps policymakers legitimize hard security measures and delegitimize militant power contenders. After reviewing empirical evidence on the limited use of force as the only strategy against terrorist threats and debunking the most common objections against negotiations with terrorist groups, the chapter then delves into the details of how such negotiations evolve as part of a wider peace process. Drawing from the conflict resolution literature and related disciplines, we discuss in particular the role of timing, trust and spoilers in such processes. The chapter concludes by looking beyond classical approaches of conflict resolution and by presenting a systemic conflict transformation approach that does not attempt to simply reduce terrorist and counter terrorist violence but engages with, and aims to transform, the underlying structural violence and oppression that often form the context in which terrorist violence occurs.

While this chapter builds on the predominant literature on terrorism and thus looks at the phenomenon mostly from the perspective of governments, we acknowledge the conceptual bias in that approach and provide an insight into the theoretical debate that challenges the simplistic view of terrorism as a non-state phenomenon and a conflict between legitimate state actors and illegitimate power contenders.

Keywords: terrorism, peace process, conflict prevention, negotiation, dialogue, conflict transformation
“The United States gives terrorists no rewards and no guarantees. We make no concessions. We make no deals.” President Reagan’s uncompromising stance in the face of the American hostage crisis in Lebanon in the 1980s is only one of countless statements that illustrate the categorical refusal of many political leaders to use anything other than force in their interactions with terrorist groups. Their refusal is deeply rooted in the realist tradition of foreign policy, which has always put a great deal of importance on the privileged role and sovereignty of nation states and on deterrence as a central concept in the interaction with enemies. As the only legitimate authority to decide on the use of force to protect the integrity of the state and the security of the people, states secure their survival in an anarchic international system by means of power, making war both inevitable, and acceptable to deal with threats to security. The underlying assumption is simple: a government that has consistently carried out its threats and has taken a firm stand in the face of an external challenge is seen as strong and uncompromising and must not fear another challenge. However, a government backing down is, according to that understanding, seen as irresolute or weak and therefore more vulnerable to threats from power contenders on the inside or the outside. Especially after 9/11, and following the declaration of the “War on Terror” by President George W. Bush, this belief in reputation and the focus on the use of force to contain terrorism became apparent across all branches of policy. His principled demand that “no nation can negotiate with terrorists, for there is no way to make peace with those whose only goal is death” started to underpin not only the US counterterrorism policy but resulted in a global trend along the line of what Ole Waever had described a few years before as “securitization.”

Although history books are filled with examples of governments which have failed to solve the problem of terrorism exclusively with hard security measures, the use of force is still widely accepted and counterterrorism by the armed forces continues to remain the preferred option for policymakers who wish to see the armed forces in a key role when responding to terrorism. The strategy against ISIS, the most recent transnational terrorist challenge, was no exception in that regard, with the international alliance pursuing a large-scale military campaign in Iraq and Syria and agreeing to rule out talks. Amongst many political leaders and their realist adepts, fighting ISIS militarily was seen as an absolute necessity and the strategy with the widest public appeal in light of some of the horrors deliberately generated by the group. Today, with ISIS believed by many to be “largely defeated,” it is also viewed as a successful war strategy and the continuation of what a considerable number of predominantly conservative politicians from former President George W. Bush (“mission accomplished”) to President Donald Trump see as an overall successful counterterrorism strategy in Iraq. However, their optimism is questionable. Just like the forced surrender of the Liberation Tigers of Tamil Eelam (LTTE) did not eliminate the underlying grievances that gave rise to the LTTE’s separatist campaign in the first place, a military defeat of ISIS – if at all a realistic outcome – will also not obliterate the breeding ground for new recruitments by terrorist networks and cells. As long as the underlying grievances of the Sunni community remain in place and as long as the powerful ex-Baathists and Saddam Hussein’s former army and intelligence officers are not separated from the jihadists, the terrorist threat of ISIS or a potential successor organization is likely to continue.

There is strong empirical evidence that suggests that military force alone is rarely the most promising path to counter terrorist threats. A comprehensive historical analysis by Seth Jones and Martin Libicki finds that only seven percent of all terrorist groups since 1968 have ended because of military defeat. While their findings have to be taken with a grain of salt due to their rather inclusive criteria of what constitutes a terrorist group, their study nonetheless provides considerable evidence to suggest that governments need to look beyond mere military means when faced with terrorist challenges. In this chapter, we will explore some of these alternative pathways.
Starting from the assumption that both terrorism and its effective prevention can only be understood as part of a wider (political) conflict and in combination with surrounding structural power relationships, we look beyond hard security measures and examine approaches from the field of conflict prevention and related disciplines, that not merely suppress terrorism as a symptom and an unpolitical act of violence but aim to resolve or transform the underlying structural and political conflict.

However, before delving into the depth of the conflict transformation literature and its coverage of terrorism as a political and social phenomenon, we must present a caveat in our analytical approach, or a conceptual bias, to be more precise. As we explain in the following section, the term “terrorism” must be looked at with considerable caution. As an attributive term, it is often used within the political sphere to challenge the legitimacy of the use of force by “others,” whereas the use of force to fight militant power contenders is considered legitimate in comparison. This approach tends to throw all forms of (armed) resistance, including resistance against all forms of oppression and autocracy, into an egalitarian basket of “illegitimate action,” resulting in a simplistic perspective on terrorism as a conflict between legitimate state actors and illegitimate power contenders. However, the instruments of terror are neither restricted to non-state actors (actually the roots of the term terreur were related to a mode of state rule in the 1790s) during the French revolution, nor can state actors as such claim more legitimacy for themselves, if they flagrantly violate the human and civil rights of their people or parts thereof.

Most literature in the field of strategic studies and conflict resolution – less so in the field of conflict transformation and peace studies – is constrained by a focus on “subnational groups or activists.” This literature looks at terrorism mostly from the perspective of governments and states while neglecting terrorist activities which are the responsibility of state actors. Sociological depth of analysis can be found only in exceptional cases, especially where a distinction is made between actors representing grievances of a larger social, ethnic or religious group, and actors who represent a sectarian extremist ideology or just themselves. For the purpose of this chapter, we have to build on what the predominant literature on terrorism is offering – an understanding of terrorism as a non-state phenomenon.

To illustrate the applicability of such narrow understanding in the context of terrorism and conflict transformation, this chapter will use the example of one specific type of conflict, namely conflicts between a government and a non-state armed group that enjoys significant political support and uses terrorist means to achieve its goals. Although the lines between the oppressor and the oppressed and between what we usually refer to as “terrorism” and other forms of violence can be blurred in such conflicts, this chapter uses the term “terrorist” predominantly as a label for the latter. We do so for illustrative purposes and in order to make the content of this chapter more compatible with the overall purpose of the Handbook of Terrorism Prevention and Preparedness.

Widening the Scope: De-exceptionalizing Terrorism

Definitions of terrorism - and the way governments deal with it - have come a long way since the first attempts by realist scholars to bring structure into a concept that differs so widely with regard to actors, means, and goals. In The Routledge Handbook of Terrorism Research, there are no less than 260 definitions aiming to delineate the terrorist phenomenon. They encompass everything from the “lone wolf” actor killing civilians with a machete in the streets, to the organized non-state armed group using guerrilla strategies in civil wars. They also include loosely organized groups using sophisticated, coordinated cyberattacks against governments, and authoritarian regimes engaging in state terrorism against representatives of armed groups or civil society. There is also a broad spectrum of opinion with regards to the goals of terrorism. Following the work of Bruce Hoffman, Jerrold Post et al., Jeff
Victoroff, and William Donohue distinguish between three major ideological perspectives of terrorism, whose representatives differ with regard to both their objectives and their use of violence to achieve them. The “nationalist-separatist” type (e.g., the Provisional Irish Republican Army, the Basque ETA, the Kosovo Liberation Army) seek to gain self-determination in the form of increased autonomy or outright independence, based on ethnic or political criteria for a territorially defined entity and in opposition to what is considered to be illegitimate, foreign rule. Their violence is “typically planned, only used as necessary, and more likely to be directed away from harming innocents.” The “social revolutionist terrorists” (e.g., Hezbollah, The Revolutionary People’s Liberation Party (Dev Sol), Italian Red Brigades) seeks to change the existing social, political or economic order and uses violence to gain public support for its cause and to pressure the authorities to compromise and make concessions. Since the attainment of their goal is contingent on public support, they are likely to avoid levels of violence that would jeopardize public support. Finally, “religious fundamentalist” (e.g., the Islamic State) terrorism aims to cause maximal damage and destruction to a type of rule that is not based on its narrow and questionable interpretation of religion. It is exercised in the pursuit of a theological order with the goal of attaining religious recognition and rewards in afterlife.

All of the above examples are embedded in vastly different social, political, economic, and human realities shaped by a wide range of conflicts and grievances. Yet, despite their distinctiveness and their political and social origins, their existence is all too often subsumed under the buzzword “terrorism” and their actions reduced to nothing more than “a spectacular act of violence, essentially devoid of political and social meaning.” Due to this homogenization and trivialization of individual realities and the refusal to understand terrorism as a complex phenomenon with political viewpoints, responses to terrorism have often failed to take the crucial role of context into account, and have been directed at what was considered a single identity and a homogenous category of violence. However, to effectively prevent terrorism, we need to take a more holistic approach and accept it as a fluid and open concept that can only be understood in its specific social and political context and along with potential counterterrorist violence and the surrounding structural power relationships in which they are embedded. By adding this complexity and by embedding terrorism in its context, we dismantle what has been referred to by constructivist scholars as a “terrorism discourse” and turn the “spectacular act of violence” into one of the various practices of dissent and protests that individuals and groups in conflicts engage in. Once terrorism is deexceptionalized, we are left with nothing more than a series of conflicts that are only brought together by their designation as terrorism and the government’s response to them in the form of counterterrorism.

Instruments aiming to prevent, resolve, contain or mitigate the negative consequences of such armed conflicts should thus play an important role in any terrorism prevention strategy. The most common of these are conflict prevention, conflict resolution, conflict management, conflict transformation, peacebuilding, and reconciliation. They entail everything from short to long-term activities, tackle direct and structural violence and are applied preventively before the outbreak of violence, during wars, and in post-conflict settings where peace is still fragile and the re-emergence of violence is likely. On the one side of the spectrum are targeted and often more short-term interventions to stave off impending violence, to prevent escalation, or to stop continuation of armed conflict. Typical instruments include early warning systems, peacekeeping activities, confidence- and security-building measures, or negotiation support that helps parties analyze, question, and potentially reframe their positions to facilitate an agreement where the conflicting parties cease to use arms against one another (e.g., ceasefire) and ideally resolve their basic incompatibilities (e.g., in the form of a comprehensive peace agreement). On the other side of the spectrum are broad, long-term strategies that seek to address and transform the structural root causes of violence typically by promoting development, strengthening the rule of law, reconciling former enemies, advancing
minority rights, and by creating inclusive societies. Ultimately, these initiatives aim to change behavioural and attitudinal root causes of conflict and strengthen the institutional and social mechanisms that help transform conflicts constructively and peacefully and make societies more resilient to the causes of violent conflict.

Practitioners and scholars have long been at pains to precisely define and demarcate the concepts of conflict prevention, conflict resolution, conflict management, conflict transformation, or peacebuilding. As of today, there are still many different understandings of what these concepts entail and what distinguishes them. This chapter does not intend to address this issue. Rather than shedding more light onto the conceptual debate, we will discuss those components that we deem particularly relevant for terrorism prevention. One such element that is inherent to almost all approaches across the field is the instrument of “talking.”

Talking is not only vital for strategic negotiations in conflict resolution and prevention, but is also the central concept in long-term dialogue initiatives that aim to transform political and social conflicts constructively and nonviolently. Although rarely used by scholars as an academic concept in the context of terrorism or civil conflict, and for a long time rejected by both scholars and policymakers as an acceptable policy response to terrorism, approaches that are based on talking can prove a valuable addition to existing approaches of terrorism prevention.

“A Walk with the Devil”: Why Governments are Reluctant to Talk to Terrorists

Of course, governments cannot prevent or effectively deal with terrorism just by talking. An effective strategy also requires firm security policies, effective intelligence and, in some cases, hard military power. Ultimately, however, there are often no viable alternatives to entering talks. According to Elizabeth Lydia Manningham-Buller, the former Director General of MI5, terrorism can only be “resolved through politics and economics, not through arms and intelligence, however important a role these play.” There is strong empirical evidence to support her claim. The above-mentioned study by Jones and Libicki finds that 43 percent of terrorist groups since 1968 ended in a transition to a political process. Audrey Kurth Cronin, who looks at six possible ways terrorists groups could end - negotiation, success, failure, reorientation, decapitation, and repression - comes to the same conclusion and finds that negotiation is the most likely way for terrorists groups to come to end the use of violence. Of course, this is not to say that talking to terrorists is neither difficult nor morally hazardous, but in cases where the “terrorist” movement enjoys significant political support and the conflict parties are interested in exploring political solutions, it has often proven to be the right thing to do and the most promising way to end violence and save lives.

Yet, when political leaders contemplate the idea of talking to terrorists, they face a number of arguments against doing so. Probably the most common amongst these is the assumption that terrorism inspires more terrorism. By talking to terrorists, the narrative goes, governments allegedly give in to violence and reward those who use it, thereby encouraging other actors to engage in terrorist strategies themselves as it is portrayed as a legitimate and promising means to achieve their goals. Furthermore, terrorist groups could mistakenly perceive the offer to talk as a sign of the government’s weakness and as an encouragement to further escalate violence. Once negotiations have started, the effort to increase leverage and negotiate from a position of strength is said to serve as an additional multiplier of violence. A recent example of this phenomenon can be found in Afghanistan, where the Taliban have looked to increase negotiating leverage through battlefield gains in their talks with the US, contributing to a spike in violence and numbers of casualties unprecedented since 2001.

Secondly, it is often argued that involving terrorist groups in a negotiation or a dialogue could give them publicity and elevate them to the status of the (sole) legitimate representative of a constituency or a territory. Unlike states, many terrorist groups lack formal accountability to a constituency and can hardly be held accountable, and are thus believed to be less likely to
abide by international law, norms or principles. Transferring legitimacy to terrorist groups as the most extreme representatives of a certain claim might at the same time weaken the norm of nonviolence and undermine more moderate representatives of that claim who have pursued political change through peaceful means. Powell mentions the example of the talks between the Pakistani government and the Pakistani Taliban, which conveyed the impression of the Taliban was an actor strong enough to sit at the same table as the military leadership of a powerful state. This not only solidified support for the Taliban among its followers but also suppressed “the voices of resistance from the civilian population living under their authority.”

A third very common objection to talking to terrorists is that they are assumed to be irrational psychopaths. Engaging with them would not only be immoral and unethical, but above all pointless. This argument is particularly prevalent in the discussions around the engagement with Salafi jihadi armed groups and other religious extremists, who are often depicted as irrational and erratic adversaries detached from reality and pursuing maximalist and non-negotiable goals. Unlike revolutionary or nationalist terrorists, who “behave as rational actors facing extreme power asymmetry” and thus must “act within a set of strategic limitations…if they are to avoid alienating wider society,” ideological terrorists “do not seem to be constrained by such rational strategic limitation.”

While there is some validity in all of the above arguments, they often do not hold when scrutinized in more detail. Firstly, as we will see below, they are either not supported by empirical evidence, or rely on flawed understandings of key concepts. Although popular among policymakers, the argument that talking to terrorists encourages more terrorism seems to be largely unfounded in empirics. It is based on the crucial misconception that mistakes talking with giving in. While giving in to terrorists’ demands can indeed be seen as problematic and as a trigger of additional terrorism, the simple act of talking is not. When a government merely talks to terrorists, it does not automatically concede to their demands, but rather shows willingness to learn about the terrorists’ (legitimate) interests with the intention to come to an agreement in which neither side needs to give in. It is thus “not the act of negotiating that encourages or discourages further terrorist blackmail; it is the terms of the negotiated agreement.” The argument that talking rewards violence and encourages more violence is further flawed by the fact that talking often occurs when parties have temporarily halted violence, thus potentially turning talks into a concession that rewards the end of violence and not its use.

Second, the argument that talking to terrorists would elevate them to the status of a legitimate representative of a constituency is problematic for two reasons. On the one hand, the argument falls victim to a flawed or biased understanding of the concept of legitimacy. According to Mark Suchman’s constructivist definition, legitimacy needs to be understood as “a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs and definitions.” Once we adopt this definition, the legitimacy of states and non-state groups is not predetermined but dependent on whether their actions are deemed appropriate by a social group. Hence, the state does not automatically confer legitimacy to any group it talks to, but non-state armed groups might acquire legitimacy through their own actions, for example by abandoning violence during talks and pursuing nonviolent means to achieve their goals. On the other hand, it makes the implicit assumption that accountability and legitimacy are a prerequisite for talks.

Yet, there is a long list of illegitimate governments that are not compliant with the rule of law and human rights and that have used horrific violence against other states or against their own people, but are still being talked to. At the same time, there is also a significant number of non-state armed groups which abide by international law, norms or principles but are nonetheless categorically excluded from talks. This includes a number of groups which still fall under categories of designated terrorist groups according to international lists, despite

80 HANDBOOK OF TERRORISM PREVENTION AND PREPAREDNESS
having changed their strategy regarding the use of force, due to a growing understanding that their case of resistance would be strengthened and more tolerated if they adhered to standards of law in order to get rid of sanctions, including lifting of proscription.49 The boundaries are sometimes fuzzy, especially in protracted social conflicts, where terrorist groups may more or less officially represent the hardline factions of larger social movements. Hezbollah and Hamas, for example, have “military arms” but are designated terrorist organizations in their entirety. Hezbollah, however, has even become part of an internationally recognized coalition government in Lebanon, whereas Hamas – although not recognized – has de facto ruled Gaza city as a local government with all related authority for the Gaza strip.

Third, while there certainly are irrational, erratic psychopaths among the ranks of terrorist groups, most terrorists are, by and large, surprisingly normal in terms of their mental health. Based on intensive study of biographical data on 172 participants in a jihadi movement, Marc Sageman found little evidence of personal pathologies or mental disorder.50 While it may not always be a rationality that we immediately understand, most terrorists are “neither crazy nor amoral but rather are rationally seeking to achieve a set of objectives.”51 Disregarding these arguments, governments throughout the twentieth century have time and again fallen into the trap of escalating repression and violence and categorically ruling out talks with an opponent they labelled “terrorists,” only to belatedly realize that negotiations would have been the only way out.52 A salient example of this was the British government in its war against the Irish Republican Army (IRA) between 1919 and 1921, where they first heavily escalated repressive violence with the goal to “terrorize the terrorists” only to realize later that no amount of coercion would resolve the “Irish Question.”53 Ultimately, the parties engaged in secret talks followed by open negotiations, which finally led to the Anglo-Irish Treaty. However, the lessons from the experience in Ireland did not seem to affect the handling of similar situations later on. The British met both the nationalist Palestinian uprising (1936-1939) and the Mau Mau uprising in Kenya (1952–1960) with repression and violence, and only when this strategy proved unsuccessful did the British government withdraw or start negotiating. In a similar manner, it took the French government more than five years of a bloody war against Algerian nationalists to realize that there was no military solution to the conflict. In June 1960, French President Charles De Gaulle secretly met with leaders of the Front de Libération Nationale (FLN), initiating a series of talks that resulted in a third party mediated negotiation that led to the Evian Accords of 18 March 1962 and ultimately the recognition of full sovereignty and the right to self-determination of Algeria.

The US has been reluctant to talk openly to non-state armed groups it characterizes as terrorists. However, unlike what the quotes from President Bush in the previous section would suggest, the mantra of not talking to terrorists is not as ubiquitous as it used to be. After long counterinsurgency campaigns in Iraq and Afghanistan, US negotiators followed the advice of General David Petraeus to also talk to those “with American blood on their hands” and started talking with the Sunni insurgents in Iraq, and the Taliban-affiliated Haqqani network in Afghanistan.

**Talking to Terrorists: Process, Concepts and Actors**

Talking – understood as a conversation between individuals – includes a broad spectrum of different types of conversations between political actors in the context of terrorist violence. In this chapter, we distinguish broadly between strategic negotiations aimed at resolving a conflict and ending direct or physical violence and talking in the form of long-term dialogues that aim to constructively transform a terrorist conflict and the underlying structural root causes. While the latter is still a rather marginal phenomenon in the field of terrorism prevention, the above examples show that the former, even if reluctantly, is finding its place in the toolbox of governments that face terrorist violence in a civil conflict. But how do such negotiations take
place? What are the key concepts, who are the central actors and what are their goals? The next part of this chapter elaborates on these questions, discusses various aspects of negotiations with terrorist groups and shows how traditional concepts and instruments from conflict prevention and resolution practice can also be applied in conflict contexts marked by terrorist violence.

**The Process of Negotiations**

There is no such thing as a blueprint for negotiations with non-state armed groups in conflicts marked by terrorist violence. Such processes are inherently complex, organic and non-linear. Progress is slow and incremental - one step forward is followed by one or sometimes two or three steps backwards. Long periods of stalemate are interspersed with setbacks and breakthroughs. Consequently, parties and mediators require a high degree of improvisation and constant adaptation as the talks develop. It is for this reason that Richard Holbrooke, one of the brokers of the Dayton Agreement (which brought peace to Bosnia and Herzegovina in 1995), compared such talks to jazz: “It’s improvisation on a theme. You have to know where you want to go, but you don’t know how to get here.”

Different peace processes thus have different numbers and types of phases. Former South African president F.W. de Klerk, for example, divided the talks between the South African government and the African National Congress (ANC) into three broad stages. The talks started with an exploratory phase, continued with informal talks that removed the most pressing obstacles and prepared structured negotiations, and ended with formal and representative negotiations that resulted in a new constitution. Yair Hirschfeld, one of the architects of the Oslo peace process, structured the process into four phases: fact-finding, authorization for the talks, legitimization of the channel, and breakthrough from backchannel to official talks.

Despite their unpredictability and context specific nature, talks with groups labelled as terrorists require a robust architecture and a clear, yet flexible strategy. Both scholars and practitioners have therefore attempted to condense and give structure to the complexity and non-linearity of such processes, identifying a series of distinct stages parties must go through in a successful process.

In his 2014 book, *Talking to Terrorists: How to End Armed Conflicts*, Jonathan Powell sketched out the broad contours of what such a framework could look like. Taking into account experiences from past negotiations and looking at evidence from research, he outlined several steps that are inherent to almost all of these processes. At the very beginning stands the difficult and often dangerous task for government negotiators or third party mediators to make contact with the enemy, who in the case of clandestine armed groups is often decentralized, operates in a covert manner and does not officially maintain a representative headquarter. Reaching out to the leadership of those groups and persuading it to meet and make initial personal contact is not just a prerequisite to start a dialogue or a negotiation. Travelling to their territory and putting your political reputation, or even your life in their hands, also constitutes an act of confidence that builds trust and respect. Having established that contact, the next stage in the process requires the establishment of a channel of communication between the two sides which is safe, and in which everyone has confidence. Such informal backchannel talks help develop working trust in each other’s seriousness about making peace without conferring any legitimacy to terrorists and their demands. They are usually conducted by members of intelligence agencies because there is a very high need for both secrecy and deniability at this stage of the process as both sides still engage in a process of “villainization” of the other party. If the talks would be made public at this stage, the negotiators on both sides would risk losing credibility in their own communities, which could discredit them as hypocritical or accuse them as traitors.

At some point, however, if talks are to progress and fulfil their purpose of reducing terrorist violence and creating sustainable peace, backchannels must turn into official negotiations. We
will discuss below under what circumstances such a transformation is most likely. As in most peace processes, negotiations with terrorist groups are unpredictable, long-term processes that demand a high level of resilience, patience and steady determination by everyone involved. Yet, given the nature of the counterpart, the issues at stake, and the power asymmetry between the negotiating parties, they are also fundamentally different from approaches of classical diplomacy in peace processes.

Negotiations are also not about winning an argument or proving each other wrong. They do not solve the causes of the conflict immediately, which can only be achieved politically once the armed group has put down its weapons and managed to win support in democratic elections. Negotiations are primarily about working towards a common understanding, building trust and finding common ground with the opposing party and – sometimes even more difficult – also finding support within one’s own constituency. The central element of this endeavor is not so much the resulting agreement but the process itself, where the “parties engage in a systematic process of mutual reassurance, based on responsiveness and reciprocity, in order to build and maintain trust in the peace process and the peace partner.” To make this possible, it is vital that the process is constantly moving, however slowly, as any breaks or interruptions could create disorientation or a vacuum that may quickly be filled with violence. Hence, to prevent negotiations from breaking down, mediators, rather than discussing issues sequentially and running the risk of reaching a deadlock over an intractable issue, often rely on a parallel structure of different issue arenas. This architecture not only allows for trade-offs between different concessions on different issues but also reduces the risk of “process fatigue” among the parties and their constituencies. The work of the main negotiators is further facilitated by a number of ad-hoc or permanent working groups of experts that meet alongside the main negotiation table and work out the technical details of the agreement.

A peace process does not end with an agreement being signed nor does it solve the causes of the conflict. An agreement is thus rather the beginning of a process that gives “parties the necessary building blocks to start working towards a peaceful society.” Trust, reconciliation, justice, and peace can only be achieved if both sides deliver on their promises and implement the provisions of the agreement. These provisions can include political changes, disarmament, demobilization and reintegretion (DDR) measures, or security sector reform that creates an army and a police force that is accepted by both parties and enjoys legitimacy among all constituencies. In most cases, a joint or independent commission is appointed to monitor the implementation of these provisions and the structure of the armed group is kept in place in order for its command and control system to ensure implementation of their side of the agreement.

Further guidance for negotiations with terrorist groups has been provided by William Zartman, who identifies seven stages in the pathway to a successful peace process with terrorist insurgents. The first of these is “mutual recognition.” For a process to take off, it is essential for parties to acknowledge each other’s existence and equality and to recognize the underlying grievances of the conflict as well as each party’s role in their cause.

In a second stage, the parties must put an “end to the fighting.” Zartman calls this move a “down payment on the resolution of the problem” as parties renounce violence as a means to direct attention to their grievances and show the willingness to move the underlying problem from the battlefield to the political arena.

The third stage - the end of violence - should coincide with a “critical shift to forward-looking negotiations” in which parties change their focus away from backward-looking negotiations on ending violence and focus on developing positive, cooperative relations to handle the underlying issue that gave rise to terrorism.

The fourth stage should be dedicated to “establishing mechanisms, relations and institutions” that manage the underlying conflict, work to prevent future eruptions of violence and build channels for future cooperation. These can include constitutional revisions, a new
political system, changes to the security apparatus or the strengthening of institutional reconciliation and transitional justice. This institutional renewal should be closely followed by stage five, the “establishment of measures of accountability.” This references domestic and international criminal law or traditional customary practices that aim to eradicate the notion of impunity and serve as a normatively acceptable replacement for revenge – all the while trying not to jeopardize efforts of reconciliation and forgiveness.

The latter should be supported by the sixth stage - a “recreation of the record of the past” that aims to change the historical narrative and provide the social basis for the transformation of the conflict. Writing and teaching of history can no longer serve as an instrument of mobilization and conflict on each side but should become a vehicle for revising historical events, confronting the past in a critical way and ultimately promoting a common history.

Finally, these efforts should all culminate in the seventh and final stage of Zartman’s framework of successful conflict transformation: the long-term goal of a “common project” that is based on collaborative relations, a shared destiny and ultimately a shared identity.

**Trust: Prerequisite and Objective**

Irrespective of the number and types of stages, there are some concepts that are crucial to all negotiations and dialogues in conflicts that are marked by terrorist violence. One of them is the trust between warring parties. While trust and confidence are often the first victims of conflict, their destruction usually lasts well beyond the end of violence. Deep-rooted, protracted conflicts are characterized by a profound mutual distrust that becomes deeply embedded in history and reproduced in culture and societal narratives. To resolve such conflicts and successfully transform adversarial relationships into peaceful cooperation, trust is a central requirement. Without some degree of mutual trust into the potential of a collaborative process, parties to a conflict cannot and will not enter into talks, as they fear that the other side will take advantage of their openness and truthfulness. Since trust in one another is a learning process, it is thus trust in the process of talks and negotiations and the mutual acceptance of, and compliance with, clear and transparent ground rules that are necessary in the first place. At the same time trust is also an important effect of constructive talks. As parties enter a peace process with deep suspicion of one another, talking can help them build trust, understand the opponent’s (and their own) interests and explore the other party’s flexibility and trustworthiness at relatively low costs and under conditions of deniability.

In the long run, of course, mutual trust among the negotiators is not sufficient. The trust that emerges from learning processes of those who negotiate must transpire to the wider public in order to enlarge the support for the process within the parties’ constituencies. According to Herbert Kelman, parties to a conflict can overcome the basic dilemma of mistrust when talking in violent conflicts through a process of successive approximations of commitment and reassurance. In that process, the parties initiate communication under conditions of deniability, and at a level and in a context that represents a relatively low degree of commitment and risk, before they slowly and gradually move toward official negotiations, ultimately and ideally culminating in a binding agreement. Kelman mentioned the 1993 Oslo talks between the Israeli government and the Palestinian Liberation Organization (PLO) as an example for such successive approximation of commitment and reassurance. After exploring possible options under conditions of deniability and low risk, the talks gradually led to the “development of new ideas that the participants brought back to their respective leaderships, to testing of the seriousness of the other side, and to building of mutual working trust, which eventually transformed the talks into official negotiations, culminating in an agreement based on formal mutual recognition.”

Another example is the US-Taliban negotiation process in 2019-2020, which took more than nine months for a comparably small set of issues to agree on because
the Taliban negotiators had to continuously consult their superiors for each single step because of concerns that the movement could fall apart without full internal consensus.

**Timing: The Perception of a “Mutually Hurting Stalemate”**

While talking may be the right thing to do, it is not always the right time to do so. For negotiations to take place and to lead to a sustainable reduction in (terrorist) violence, timing is crucial. However, unlike in traditional interstate warfare where negotiations usually only started once military fighting had come to an end and had resulted in victory and defeat, today’s interstate conflicts often do not have a clearly identifiable moment at which adversaries naturally start talking. Negotiations in today’s asymmetric protracted conflicts often take place while fighting is still ongoing or merely suspended. Identifying the right moment in such a scenario is thus often a complex endeavour and a matter of assessing the various options available. If one or both parties realize that continuing the fight entails more risks than entering into talks, they might revisit their current approach.

A conflict actor that is close to being defeated will possibly be more reluctant to accept, let alone offer negotiations as this would either further substantiate claims that the group was losing or – with nothing left to lose – might also escalate violence for one last all-out battle. The same logic applies to conflict actors that are doing well enough on the battlefield to believe that they can best attain their aims by violent means. For them, offering or accepting talks is neither a very likely nor promising scenario. History has shown that a realistic chance for talks between a government and a non-state armed group lies in between these two scenarios. Parties to a conflict are most likely to resort to talking when they find themselves in a deadlock that is painful to both of them (although not necessarily to the same extent or for the same reasons) and from which neither side can attain victory. Faced with that uncomfortable and costly predicament, generally referred to as a “mutually hurting stalemate,” parties come to realize that their goals are unattainable by further violence and possibly better achieved by pursuing an alternative line of action.

Zartman was the first to put into writing the concept of the “mutually hurting stalemate” and the assumption that a conflict can reach a “ripe” moment to initiate a negotiation process. Importantly, what makes the parties agree to hold talks is not so much the objective fact of a military stalemate in the form of casualties or material costs, but rather its subjective perception and the inability to bear the cost of further violence and escalation. However, this subjective perception of a “mutually hurting stalemate” is, on its own, not sufficient to push parties into negotiations. For adversaries to talk, there must also be a pull factor in the form of a perceived “mutually enticing opportunity” that provides the parties with an attractive alternative to fighting that allows them to achieve their core goals. Without such a “mutually enticing opportunity,” negotiations and the subsequent agreement remain unstable, as the 1984 and 1999 Lusaka Agreements or the 1994 Karabakh ceasefire between Azerbaijan and Armenia illustrate.

Both the “mutually hurting stalemate” and the “mutually enticing opportunity” should not be understood as fixed moments on a linear timeline with each side waiting passively until they arrive and convince parties to negotiate. Instead, the limits of the bargaining space constantly fluctuate and opportunities to talk appear and disappear. Meanwhile, the frequent assessment of a Best Alternatives To a Negotiated Agreement (BATNA) has become a well-known principle in the strategizing of talks and negotiations also for many armed groups. A “mutually hurting stalemate” and a “mutually enticing opportunity” are neither self-fulfilling nor self-implementing but must be seized, either by the parties and their leadership themselves or through the persuasion of an external mediator. The latter can influence the parties’ “negotiability” by increasing the size of the stakes and by projecting a situation where failing to enter a negotiation process would hurt the parties more than continuing the conflict. The
role of the mediator, however, remains often a delicate one and requires an enormous amount of caution. Especially when parties are not ready, active mediation can end up doing more harm than good and “even a well-intended engagement can lead to a splintering of groups, which in turn may lead to an increase in the use of violence.”

The argument around a “mutually hurting stalemate” and a “mutually enticing opportunity” has been used widely in the literature on conflict resolution and is further substantiated by numerous empirical examples. According to James Goodby’s article *The Timing of Peace Initiatives: Hurting Stalemates and Ripe Moments*, the lack of a “mutually hurting stalemate” explains why there was no chance of a mediated settlement in Bosnia in the summer of 1994. Yet a negotiated agreement was achieved at the end of 1995, after large-scale NATO air strikes created a military stalemate in which no party continued to believe it could achieve its goals through war. Similarly, Zartman sees the absence of a “mutually hurting stalemate” as the primary reason, why mediation efforts of the US government did not bear fruit in the Ethiopia-Eritrean conflict in the early 1980s and the early 1990s nor in the Southern Sudan conflict in the 1990s.

Using a “mutually hurting stalemate” as an initial ignition for talks can be particularly problematic in conflicts marked by terrorist violence. Due to the inherent asymmetry and the military superiority of the state in such conflicts, it can be “difficult for state leaders and officials to accept that they are unable to defeat a small group of what they often consider to be criminals and social outcasts.” However, that does not mean that a “mutually hurting stalemate” is not possible in such conflicts. On the side of the terrorist group, it is equally difficult to recognize the perception of a ‘mutually hurting stalemate’ as it requires the group and its leaders to learn from their experiences of suffering and lack of gains. Brutally honest self-reflection is the only way to better “distinguish between their inherent position as the militarily weaker party and a position in which victory through violence is impossible.” However, if both the government and the non-state armed group perceive the conflict to have arrived at a stalemate and to have reached a ripe moment where none of the parties seem to be making advances to decide the situation in their favor, talks become a realistic possibility. This is what we have witnessed in 2019-20 in Afghanistan, where after almost two decades of war, the Afghan government, the Taliban and the US have shown willingness to explore viable solutions to the conflict and to engage in talks about how to end the conflict through an agreement.

Although important, a “mutually hurting stalemate” and a “mutually enticing opportunity” are not the only entry points for negotiation. There are also a number of external conditions that can create momentum for entering talks. One example is a major geopolitical shift as experienced with the end of the Cold War or the rise of jihadi terrorism and the subsequent “War on Terror.” Both had a favorable impact on the chances of successful negotiations with terrorists. The 9/11 terrorist attacks, the March 2004 Madrid train bombings, or the 7/7 attacks on London’s public transport, for example, did not only reduce the space and political support for other armed groups in Europe. The willingness of Islamic extremist to kill people on such a large scale also changed the public perception of terrorism. The general disgust about these acts made it difficult for the IRA or ETA to go back to terrorist violence. It left them with less legitimacy, justification, explanation or support. Powell identified a number of other entry points for mediation activities, including changes in the leadership structure of the conflict parties, the arrival of a new external mediator or natural disasters.

**Spoilers, Violence and how to Deal with these**

Negotiation processes during wartime are long, complex, and uncertain, with groups repeatedly having to reshape the process, reevaluate positions and chances of achieving their goals. Irrespective of whether such talks are successful and whether they result in a reduction or even
a complete cessation of violence that is beneficial to both conflict stakeholders and the wider population, the process and its results almost inevitably create losers. These can be groups, leaders or factions who feel excluded from the process, whose demands are not (or not sufficiently) addressed in the agreement, or who have other (e.g., material) incentives for the continuation of the conflict.

To understand how such situations emerge, we first need to get rid of two flawed assumptions that have so far prohibited a comprehensive examination of the effects of negotiations with terrorist actors - first, the dyadic two-actor model of conflict, and second, the ideological homogeneity of terrorist groups. A great deal of the civil war and conflict resolution literature – and up to this point also this chapter – has assumed a simple two-player model with a government and a single, unitary (terrorist) opposition as the primary combatants and only actors in an eventual peace process. However, this very rarely reflects the reality of conflicts. Governments in civil wars usually fight multiple conflicts with several opponents simultaneously, each of those again a conglomerate of ideologically heterogeneous cells and factions, with some being more moderate and others more extremist. If we consider armed non-state actors as neither singular nor ideologically homogeneous, we should expect a variety of problematic impacts if a government engages in talks with them. On the one hand, talking to one actor instantly creates outsiders in the form of other groups who are excluded from those talks, who fear that their demands are not addressed in the talks or who are just not interested in peace. On the other hand, the offer to talk might also create tension within the ideologically heterogeneous group itself, as it is usually the “moderates” who are most likely to accept the offer to talk, leaving the “extremists” in control of a terrorist organization that is now more militant than it had been before. These internal cleavages can become serious obstacles to constructive talks. Of course, they are not only restricted to the power contenders. Rebel groups are by no means less united than the government they are challenging. Ruling parties in fragile states are often not “united” themselves but represent pragmatic power deals between different factions within an ethnic or religious community. Even statutory forces can be partisan entities within internal national power games, as shown by the example of the Democratic Republic of the Congo.

Having limited or no stakes in the talks, these often marginal and less cohesive outside actors can aim to alter the process or derail it completely. In the conflict resolution literature, they are generally referred to as “spoilers,” defined as leaders or parties “who believe that peace emerging from negotiations threatens their power, worldview, and interests and use violence to undermine attempts to achieve it.” Parties labelled as spoilers may not necessarily use violence and may not always be interested in completely derailing the peace process. In some cases, their role is a productive and positive one that makes the process more fair, equitable, and inclusive, and may be closer to George Tsebelis’ concept of a “veto player” - that is, an “individual or collective actor whose agreement...is required for a change in policy.” In this chapter, however, we stick to Stephen John Stedman’s definition and focus on violent, destructive spoilers that use terrorist tactics and strategies to influence or end negotiations. It is not only in line with the topic of this chapter and this Handbook, but it also reflects the fact that terrorism in the way it is predominantly being looked at in the literature may be unique in its ability to spoil a peace process as terrorist groups or their factions see their goals threatened by peace processes which are predominantly dominated by “moderates.”

Spoilers can be inside or outside a peace process, they can vary in numbers, can seek finite goals, or seek exclusive power or can expand or contract their objectives, based on calculations of cost and risk. Terrorist spoilers may be major parties to a conflict that are not satisfied with the handling of the peace process (e.g., Hamas in Palestine or Hezbollah in Lebanon) or small, radicalized factions of larger organizations who see terrorism as the main or the sole tactic to disrupt the process (e.g., the Real IRA in Northern Ireland, after the Provisional IRA agreed to abide by the Mitchell Principles in 1997). Some actors might use violence for different
purposes at various stages. In the run-up to, or in the early stages of negotiations, groups might use violence to get a seat at the negotiation table and to demonstrate the necessity of being included in the talks and in the agreement. During negotiations, parties may use violence to increase their bargaining leverage and extract further concessions, to gain power within its own camp or to stop the talks and return to war. During implementation, violence might be used to force the renegotiation of certain terms of a settlement or to cause the complete breakdown of a fragile peace.

Examples of extremist and terrorist spoilers in peace processes are manifold. In Northern Ireland, paramilitary groups on both sides (e.g., the Real IRA, the Continuity Irish Republican Army (CIRA), or the loyalist Orange Volunteers) have used terrorist tactics to challenge the 1998 Good Friday Agreement and its implementation. Attempts of terrorist spoiling also plagued in the early 1990s the Oslo process between the government of Israel and the PLO, whereby Hamas and several other rejectionist Palestinian factions attacked Israeli and PLO forces and carried out a series of bombings on civilian targets in an attempt to end the Oslo Accords. Terrorist attacks were also used as a means to spoil the peace processes in the Philippines or in Papua New Guinea. Spoilers within and outside the Moro Islamic Liberation Front (MILF) disrupted on various occasions the two decades long negotiations that culminated in the 2014 Comprehensive Agreement on the Bangsamoro (CAB). Much smaller, but equally difficult to deal with, was Francis Ona and his small band of loyal supporters who resisted the peace process in Bougainville by attacking peacekeeping troops and assassinating Bougainville Revolutionary Army (BRA) commander Paul Bobby, who was involved in the peace process with the central government of Papua New Guinea.

The above examples do not yet allow a general verdict about the effects of terrorist spoilers on the success of peace processes. While some of the spoilers succeeded in disrupting or delaying the peace process, others did not. The literature on the effect of terrorism on the success of peace processes is equally inconclusive. While some scholars discount the role of terrorist spoilers as marginal, numerous studies find that even low-level terrorist violence can have a powerful impact on the course and outcome of peace talks. Yet there are also some scholars who found a positive side effect of spoiler attacks. In cases where there is widespread popular support for the peace talks, terrorist spoiling – rather than undermining the peace process – could “serve as a reminder of the consequences of continued conflict” and further strengthen the resolve of parties and make them “more determined in their attempts to pursue peace.” This is what happened in Northern Ireland after the 1998 Omagh bombing killed 29 civilians just a couple of months after the Good Friday Agreement had been signed. According to Cronin, effective public relations efforts by all parties managed to frame the terrorist attack as an explicit attack on peace and also deflected popular passion from the opposing side as a whole to the splinter faction that was undermining the peace process. This unified narrative made the negotiators in Northern Ireland more determined and helped transform the talks into a productive channel.

However, the vast majority of the academic work on terrorist spoiling finds a negative effect on the development or the outcome of the peace process. Looking at spoiling in 14 peace agreements signed between 1988 and 1998, Andrew Kydd and Barbara Walter found that extremists are indeed likely to be successful in bringing down peace processes if they so desire. Their analysis shows that only one in four peace agreements was put into effect after terrorist attacks had occurred during the talks, compared to 60 percent in the absence of such attacks. Analyzing a geographically coded database of terrorism in civil wars between 1970 and 2002, Michael Findley and Josphe Young arrive at a similar conclusion, finding that the use of terrorism can spoil peace processes by prolonging the duration of a war or by leading to a resumption of violence. Their findings are further supported by Andrew Reiter, who studied 241 civil war peace agreements in the post-Cold War era. He found that violent spoiling can pose a significant threat to agreements when spoilers have the military means and ability
to prevent its implementation\textsuperscript{104} All three quantitative studies are in line with a large body of theoretical and conceptual work that finds a destabilizing effect of terrorist spoilers on the ability and likelihood of people of good will to reach an agreement.\textsuperscript{105} They offer different explanations as to why this is the case. The most prominent of these explanations is the negative effect on trust, credibility and commitment. Terrorist violence by a negotiating party or one of its factions, many scholars argue, undermines an already shaky trust and creates further resentment between (or within) the groups that are negotiating or implementing an agreement. It can imply a lack of commitment to the process in its current form and reduce the willingness of the other party to continue talks with what they are now more likely to consider an unreliable partner who is unable to control its own constituencies. In the worst case, terrorist violence is used as an argument why negotiating with the other side is no longer possible and should be terminated.\textsuperscript{106} The degree to which terrorist spoiling has a negative effect on trust depends to some extent also on the phase of the peace process. While the use of force during negotiations is not atypical (e.g., the Fuerzas Armadas de Resistencia National (FARC) \cite{ArmedForces} in Colombia and the Taliban in Afghanistan were not ready to accept a comprehensive ceasefire during the negotiations), violence in the post-agreement phase is a much more serious breach of trust with more far-reaching consequences for the process.

Another channel by which terrorist violence is believed to undermine and destabilize the process is through the other party’s response to that violence. According to David Lake, terrorist violence by a non-state armed group could provoke a harsh, disproportionate response from the government in the form of more violence and other repressive measures.\textsuperscript{107} Although targeted at the perpetrators, these measures often comprise collateral damage that can radicalize “moderates” and drive them into the arms of the “terrorists,” ultimately leading to renewed interest in fighting against the government. One strain of literature looks at the issue from the perspective of group fragmentation. It argues that terrorist spoiling is not just the result of disunity and fragmentation, but can also further aggravate divisions on both sides of the negotiation table.\textsuperscript{108} On the government side, it can undermine the “moderates” who had promoted talks and invigorate hardliners that had been skeptical of talks and supported a military solution. Similarly, on the side of the non-state insurgent, the use of terrorist strategies can lead to tensions between those factions that are in favor and those that are opposed to talking.\textsuperscript{109} Finally, terrorist spoiling not only affects ongoing or past talks, but can also cast a shadow on future talks. According to Daniel Druckman, terrorist attacks during talks can constrain actors from re-engaging in public talks and make a return to talks in the future more difficult.\textsuperscript{110}

The academic literature proposes several strategies for governments and third party mediators to manage terrorist spoilers and to prevent them from having a destabilizing effect on peace processes. At the core of most policies to combat spoilers lies the attempt to raise the (opportunity) costs of violence.\textsuperscript{111} A comprehensive conceptualization of the various strategies is provided by Stedman, who classifies the strategies along a broad spectrum of approaches, ranging from accommodative inducement, to adaptive socialization and coercive punishment. The strategies remain very general and do not factor in the complexity of specific contexts. They are also not mutually exclusive, leaving governments or third party mediators with the option to employ several strategies simultaneously or consecutively.

The idea behind the “inducement” strategy is to accommodate spoilers by “taking positive measures to address grievances of factions that obstruct peace.”\textsuperscript{112} The expectation is that spoilers, after their demands have been met, are more likely and willing to join the peace process or fulfil their obligations to an existing agreement. The “socialization” strategy aims to change the behavior of spoilers by establishing a set of standards for normatively acceptable behavior by parties that commit to or want to join the peace talks. This normative framework\textsuperscript{113} then serves as a basis for assessing the legitimacy of the demands and the behavior of spoilers. A successful outcome of this strategy requires both persuasion of the value of such a normative
standard, and a “carrot-and-stick” mechanism to reward or punish spoilers’ compliance and non-compliance. A socialization strategy can be particularly effective if governments manage to build a strong coalition with civil society, other governments, and key international actors and succeed in creating a broad political climate in support of the talks while condemning terrorist violence against civilians. Of equal importance in this endeavor is the media coverage of the peace process and the way the latter is perceived by the public. If coverage predominantly focuses on negative events while ignoring positive developments, the media can exacerbate the effect of spoiling and can become a spoiler themselves. Finally, the “coercion” strategy at the other side of the spectrum “relies on the use or threat of punishment to deter or alter unacceptable spoiler behavior or reduce a spoiler’s capability to disrupt the peace process.” It can range from coercive diplomacy or the threat to reduce international support or withdraw peacekeeping forces to the actual use of force and a counterterrorism crackdown.

In practice, the most effective strategy against the spoiler problem is not to combat or manage them once they have come into play, but to prevent them from emerging in the first place. Understanding the different motives is key to develop effective tailor-made strategies to address the spoiler problem. Research has shown that peace processes are – on average – more sustainable and more effective if they are inclusive and participatory. This applies in particular to the inclusion of representatives of civil society (e.g., religious leaders, women organizations, and youth groups), which have been shown to make a successful negotiation and implementation of a peace process more likely. Research by Ricigliano, Dudouet, and Toros has shown that this positive effect is also pertinent for non-state armed groups. Expanding inclusion in their direction reduces incentives for the strategic use of spoiler violence during negotiations and has a strong potential to limit post-agreement violence. Hence, their potential actions to destabilize or derail the process (e.g., by terrorist acts) should already be taken into account when designing the peace processes and third party mediators should include all of the important players and “resist the temptation to settle for an easy agreement with moderates, …because such settlements are very likely to fail.”

Talking Transformation?

So far, this chapter has mainly looked at talking in the form of strategic, adversarial, power-based bargaining aimed at resolving a specific crisis, and “providing short term relief to pain and anxiety.” This Clausewitzian “continuation of war by other means” where each side tries to maximize its gains is, however, not the only form of talking in the context of a terrorist conflict. Other than an instrument of strategic negotiations, talking can also be communicative in the form of a transformative dialogue. A dialogue looks at the broader conflict and aims to explore, understand and eventually transform the relationships and patterns that gave birth to it in the first place. In doing so, it moves beyond the state as the only interlocutor in classical approaches of conflict resolution and negotiation and engages a broad spectrum of actors from civil society, religious groups, and other non-state actors. While power-based negotiations are usually attributed to the concept of conflict resolution, dialogue is a key concept in conflict transformation approaches. Such negotiations are seen as distinct, competing, often exclusionary forms of practices that stand in opposition and in a superior relationship to one another. However, since both forms are possible in situations characterized by terrorist violence and since they usually occur simultaneously and in a reciprocal manner, this chapter ends with a closer look at this alternative, less-frequently used, yet equally important and effective, form of talking. The concept of conflict transformation emerged as a reaction to the dominant practice of conflict resolution with its focus on ending direct violence and finding an immediate solution to the conflict while often leaving systemic violence and structural oppression in place.
Conflict transformation is based on the assumption that conflict is not necessarily a negative force but an inherent and inevitable part of human interaction and a natural expression of social difference that, if managed non-violently and constructively, can uncover and contest systemic violence and structural oppression and be a driver of social change. Hence, rather than trying to resolve or suppress conflict, the aim of conflict transformation scholars and practitioners is to transform its destructive, violent manifestation and turn it into a constructive force that reduces the oppression that generates and perpetuates underlying structural violence. Conflict transformation in conflicts that are marked by terrorist violence thus applies a holistic or systemic approach that not only attempts to reduce and de-escalate terrorist and counter terrorist violence but also goes beyond the short- to medium-term perspective by engaging with the underlying structural violence and oppression that often form the context in which terrorist violence occurs. In the tradition of John Paul Lederach, Diana Francis, and Raimo Väyrynen, conflict transformation is thus understood here as “a spectrum of degrees of change which can include, at its most ambitious, the radical restructuring of the world order but also refers to personal transformation, the transformation of relations between two or more individuals, and the transformation of means (e.g., away from violence) in a specific conflict.” As a holistic concept, conflict transformation is about reflecting on the complexity of systems and contributing to their transformation by mobilising and changing their constituting, interconnected elements. It is about changing actors, issues, relationships, structural and cultural factors, attitudes, behaviours, discourses, goals and the means to achieve them. Based on earlier work by Väyrynen, Lederach, and Toros, one can identify four areas of potential transformation in conflicts marked by terrorist violence:

1. Talking can contribute to a transformation of means whereby actors to the conflict cease engaging in terrorist or counter terrorist violence and instead start using nonviolent means to pursue their interest. Potential outcomes of this transformation range from ceasefire agreements or strategies for DDR to the use of nonviolent resistance and, ultimately, the transformation into a political party and the entry into conventional party politics. As the transformation of means often comes along with a modification of a group’s goal, it is sometimes wrongfully described as a transformation from “war to politics,” disregarding the fact that these groups have often been political from their beginnings.

2. “Relational” transformation aims to change asymmetric interpersonal relations between conflicting parties, where former enemies accept to talk to one another and create the foundation for a more balanced relationship based on understanding and trust at all levels, from the leadership all the way down to the constituency.

3. Through “personal” transformation of people’s beliefs and perceptions and supported by a process of familiarization and humanization, parties develop empathy and stop perceiving themselves only as victims and start recognizing their role as perpetrators too.

4. Finally, “structural” transformation ultimately aims to transform the economic, social, and political power relationships underlying the terrorist conflict. It is both the consequence of the transformation of means, relations, and personal transformation but at the same time also helps solidifying them. Structural transformation does not directly emerge from talking or from the peace process as such but is incentivized through the institutional framework achieved by those processes i.e., if an agreement or a constitutional change address underlying economic, social, or political inequalities, or if the transformation of the legal status of the formerly outlawed armed group removes the terrorist label and allows it to become a political party and pursue its goals with nonviolent means.
Although separated for the sake of presentation, these four forms of transformation are far from distinct and mutually exclusive. They are heavily intertwined and dependent on one another, both within and across conflict divides. The transformation of means can influence relational, personal, and ultimately structural transformation, and vice versa. Similarly, transformation cannot be one-sided and is only effective if both parties engage in the process. An armed group will in many cases only renounce terrorist means if the government puts an end to violent counterterrorist measures and a transformation in identity from a non-state armed group into a political party is only likely if the state is equally willing to transform its identity (e.g., from a centralized to an ethno-federal state or from a one-party to a multi-party system).

Finally, a sustainable transformation of terrorist conflicts is only deemed realistic if the interests and (legitimate) needs of all its stakeholders are taken into account. One crucial consequence of this systemic approach is a strong focus on the capacities of local actors. Whereas traditional conflict resolution approaches tend to focus their attention on high-level representatives and external third parties, conflict transformation researchers and practitioners see embedded local actors as the primary agents of constructive change. In their view, “decisions on the development and direction of social transformation should be taken, first and foremost, by local actors.”

Hence, rather than merely focusing on the ‘moderates’ and other obvious stakeholders within the conflict system, sustainable transformation of terrorist conflicts uses the transformative power of a broad variety of actors, including local armed actors, civil society groups, women’s groups and religious communities.

This systemic “whole of government” and “whole of society” approach of conflict transformation accounts for the fact that terrorism is part of a wider system of coercive power with several actors and perpetrators and complex chains of causality in multiple directions and amongst all associated factors. Unlike in the securitized counterterrorism logic, conflict transformation hence does not build interventions around the terrorist group as the only actor and violent perpetrator in a conflict. It allows for a wider understanding of violent extremism and terrorism as the result of structural drivers (e.g., repression, inequality, poor governance, violations of human rights, discrimination, unemployment, and foreign interventions), individual motivations (e.g., a sense of purpose, victimization, belonging, identity, acceptance, status, expected rewards, material enticements) and enabling factors (e.g., presence of radical mentors, access to radical communities and ideologies, access to weapons, lack of state presence, absence of family support). It is only once such factors are fully taken into account and the structural drivers, individual motivations, and enabling factors are tackled, that we can more effectively and sustainably prevent terrorism.

Dr Andreas Schädel is a Research Fellow at the Berghof Foundation in Germany and Advisor for Design, Monitoring and Evaluation in peacebuilding and conflict transformation projects. He has worked for the disarmament section at the Swiss Mission to the United Nations in Geneva and in various positions in the academic and financial sectors. Andreas Schädel earned his Ph.D. from the Chair of International Conflict Research at ETH Zürich with a dissertation on the role of reputation in separatist conflicts. He holds an MA in International and Comparative Studies from ETH Zürich and received his BA in Political Science and Economics after studying at the University of Zürich and at the Institut d’Etudes Politiques de Bordeaux.

Prof. Dr Hans J. Giessmann was Executive Director of the Berghof Foundation and Director of Berghof Conflict Research Between 2012 and 2019. Before joining Berghof in 2008, he was Deputy Director and Senior Researcher at the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH). His systematic research on terrorism began in 1995. At
the beginning, his research focus was primarily on the challenges for countering terrorist violence whereas his main interest shifted later to provide technical support to actors willing to enter into peace negotiations in asymmetric armed conflicts, most recently in Afghanistan. From 2009 until 2014 he was a member of the Global Council on Terrorism to the World Economic Forum, and chaired the Council in 2011 and 2012. He graduated from the Humboldt University in Berlin in 1978 (Dipl.-Phil.) and holds doctorates in philosophy (1981) and in political science (1987). In the past, he has held guest professorships in the universities in Garden City (N.Y.), Wroclaw and Shanghai and visiting fellowships at EWI in New York and EU-ISS in Paris. As author, editor or co-editor he has published more than 40 books and about 400 research reports and articles, with numerous translations into more than ten languages.
Endnotes

5 President Donald Trump in August 2019, quoted in Burke, Jason, ‘isis Starting to reassert itself in Middle East Heartlands, UN Warns,’ The Guardian, 30 January 2020. Available at: https://www.theguardian.com/world/2020/jan/30/isis-islamic-state-starting-reassert-itself-middle-east-heartlands-un-warns.
6 It is debatable if Sri Lanka can be used as an example here. Powell argues that the Sri Lankan army managed to defeat the LTTE precisely because they evolved away from terrorist strategies and transformed into a conventional combat force. Powell 2014a, p. 38.
9 The US State Department defines terrorism as “premediated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents” (see 22 US Code § 2656f).
11 Conflicts are defined here as a “contested incompatibility that concerns government and/or territory where the use of armed force between two parties, of which at least one is the government of a state, results in at least 25 battle-related deaths in one calendar year” (see the Uppsala Conflict Data Program (UCDP)).
17 Ibid., p. 438.
18 While this threefold categorization aims to illustrate the heterogeneity of an often homogenized phenomenon, it is in itself an over-simplification of the reality in which violent Islamist groups are “the product of specific, local conditions more than they are manifestations of grand, global ideologies” (Glazzard, Andrew et al., Conflict, Violent...


20 Ibid., p. 89.


22 This realisation has gained increased prominence in both research and practice. The UCDP for instance, probably the most frequently used provider of data on organized violence and armed conflict around the world, refrains entirely from using the terms “terrorism” or “terrorist” to classify violence or actors perpetrating violence. Instead, the UCDP classifies occurrences of organized violence according to the respective targets, where it distinguishes between states, representatives of organized groups, and civilians. Any attack on civilians is subsumed under the category “one-sided violence,” which the codebook defines as “the use of armed force by the government of a state or by a formally organized group against civilians.” (Cf. Eck, Kristine and Lisa Hultman, ‘One-sided violence against civilians in war: insights from new fatality data.’ Journal of Peace Research, 44(2), 2007, pp. 233-246). Although overlapping with standard definitions of (lethal) terrorism, the UCDP’s category of “one-sided violence” is much broader and by including governments of states also applies to actors which according to many definitions of terrorism cannot be considered “terrorists.”


29 Toros 2012.

30 Powell 2014a, p. 41.

31 Jones and Libicki 2008.


33 These arguments are based on the list of arguments provided by Powell 2014a and Toros 2012.

34 Cf. Schmid, Alex P. and Ronald D. Crelinsten (eds.), Western Responses to Terrorism. London: Frank Cass, 1993, pp. 311; Cronin 2009, p. 35.


36 See: Byman, Daniel, ‘The decision to begin talks with terrorists: Lessons for policymakers,’ Studies in Conflict & Terrorism, 29(5), 2006, pp. 403-414; Bapat, Navin A.,


40 Powell discusses a number of other, more practical arguments against talking to terrorism: Talking to terrorist groups could furthermore; 1) harm relations with allies and undercut international efforts to outlaw terrorism; 2) bring down the government and destabilize the political system, 3) or give terrorists a chance to rest and regain strength. Powell 2014a, p. 29. See also Fettweis, Christopher J., ‘Freedom Fighters and Zealots: Al Qaeda in Historical Perspective,’ *Political Science Quarterly,* 124(2), 2009, pp. 280.


42 As a case in point that exemplifies the difference between talking and giving in, Powell mentions the example of the conflict in Northern Ireland (Powell 2014a, p.17). Although the British government talked to the Irish Republicans, it never gave in to their demands for a united Ireland.

43 What should not be dismissed, however, is the fact that armed groups might not achieve their goals through violence but certainly manage to “be heard” because of their violence. Dudouet argues that the rationale behind turning to violent strategies is often the lack of nonviolent means available to them. Dudouet, Véronique, *From War to Politics: Resistance/Liberation Movements in Transition.* Berlin: Berghof Research Center for Constructive Conflict Management, 2009, p. 22.


47 Toros 2012, p. 45.

48 When the British government started talking with Sinn Féin, it did not make the latter a legitimate entity, particularly not in the eyes of the unionist and loyalist community.


52 Powell 2014a, p. 335.


54 Powell 2014a, p. 241.

55 Ibid., p. 77f.

56 Ibid.
It is important to note here that official negotiations should never fully replace back channels but should run in parallel to them. Back channels remain an important tool throughout the entire negotiation process as a fallback option and for confidential and informal exchanges between trusted individuals. Often, the most important issues are not negotiated at the main negotiating table but in small groups, informal sessions, walks, or coffee breaks between trusted individuals.


The former Finnish leader Martti Ahtisaari, as quoted in Powell 2014a, p. 279.


This approach also pursues the goal of enabling the transformation of a non-state armed group into a peaceful political entity. This not only helps assure the militants that they can effectively pursue their interests through nonviolent, political channels but also “generates the political will to undergo disarmament, demobilisation, and reintegration (DDR) processes and to then enter formal political channels” Dudouet 2016, p. 4.


Zartman 2005, pp. 41-49.


Neumann, Peter R., ‘Negotiating with Terrorists,’ *Foreign Affairs*, 86(1), pp. 128-138. One could also argue that a group, envisioning the risk of imminent defeat, could become even more ready to talk because it feels the risk to lose what is left to it and secure at least some stakes before being forced to surrender. An example for this argument is the LTTE. Sometimes, despair can also result in an adjustment of tactics, or in a fragmentation of terrorist groups and a reconstitution in the form of splinter groups.


Zartman 2005, pp. 41-49.


Ibid., pp. 26 ff.


Powell mentions the example of El Salvador, where 7,000 FMLN guerrilleros started their “Final offensive” in November 1989 to take the capital San Salvador. They came within 200 meters of the presidential residence. This made the Salvadorian government realize that they could not defeat the guerrilla forces militarily and that the cost of coming to an agreement had become less than the cost of continued armed conflict. (Powell 2014a, p. 175).

Toros 2012, p. 12.

Powell 2014a, p. 167.

A change in leadership can indeed make successful negotiations more likely, especially if a leader is the primary obstacle to talks. However, the academic literature is still inconclusive regarding the application of this finding on campaigns that are primarily characterized by terrorist violence. Successful negotiations with terrorists require some sort of organization as well as a spokesperson and leader. A change in leadership, however, may jeopardize this structure and may “result in a more diffuse organization that is more difficult to parley with, as its different parts chase different aims.” Cronin 2009, p.65.

An often-cited example is the case of Aceh, where the devastation by the 2004 tsunami opened a window of opportunity for the government to initiate renewed talks with GAM, which the separatists eventually accepted. Gaillard, Jean-Christophe, Elsa Clavé, and Ilan Kelman, ‘Wave of Peace? Tsunami Disaster Diplomacy in Aceh, Indonesia,’ *Geoforum*, 39(1), 2008, pp. 511-526.


90 The Continuity Irish Republic Army (CIRA) is a case in point. Opposing any deal that was not based on a united Ireland outcome, the group was left out of the negotiations over the Good Friday Agreement and used terrorist tactics to challenge its implementation.
91 This is what happened with the signing of the Oslo Accords, when the violent campaign of parts of the Palestinian movement was left in the hands of Hamas and Islamic Jihad, both of which were more committed to using terrorist tactics than the PLO. Bueno De Mesquita, Ethan, ‘Conciliation, Counterterrorism, and Patterns of Terrorist Violence,’ *International Organization*, 59(1), 2005, pp. 145-176.


See Zahar, Marie-Joelle, ‘SRSG Mediation in Civil Wars: Revisiting the “Spoiler” Debate,’ *Global Governance*, 16(2), pp. 265-280.


Stedman (2000) mentions a number of norms, including adherence to the protection of human rights, good governance, commitment to the rules of democratic competition, and accountability.

Cronin 2009.


Stedman 2000, p. 185.


Naturally, an overly inclusive approach bears the risk of making negotiating more difficult as more interests and demands need to be accommodated. See Nilsson 2008, pp. 479-495.


Lederach 2015 [2003], p. 31.


Lederach 2015 [2003], p. 31.


Hoffman 2006.


Toros 2012, p. 65.


See Dudouet et al., who list 16 examples of trajectories of armed groups towards peaceful political participation, among which the African National Congress, the Communist Party of Nepal – Maoist (CPN-M), SWAPO in Namibia, the Kosovo Liberation Army, GAM in Aceh, and the FMLN in El Salvador. Dudouet 2016.


See, for instance, Dudouet 2009.

Bibliography


Zahar, Marie-Joëlle, ‘SRSG Mediation in Civil Wars: Revisiting the “Spoiler” Debate,’ *Global Governance*, 16(2), 2010, pp. 265–280.

Web-based Resources

Uppsala Conflict Data Program: https://ucdp.uu.se/
Chapter 5

Contributions from the Military Counterinsurgency Literature for the Prevention of Terrorism

Rob de Wijk

Military establishments have learned that insurgency and terrorism are part of a broader political struggle with the population as center of gravity. Therefore, the military’s vast experience contains important lessons for dealing with terrorists in Western states. A key difference between counter insurgency (COIN) and counterterrorism operations is that insurgents rely on support of the populations whilst terrorists are individuals or isolated groups or cells without broad public support. The difference is that COIN requires a ‘hearts and minds’ campaign, whilst counterterrorism requires search and arrest or destroy tactics without causing too much trouble for the population. As the ‘hearts and minds’ campaign is a prerequisite for gaining the support of the population, this is an essential activity to prevail in a political struggle. It requires responsible leaders to abstain from harsh rhetoric stigmatization of sectors of society vulnerable to terrorist appeals and refraining from contributing to the polarization between majority and minority groups in society. Political leaders ought to respect group identities and grievances, and should take socio-economic measures to take away (some of) the grievances. At the same time, they should be aware that jihadists and other militants will try to deprive the population from a sense of security. As most insurgents and terrorists will make a cost-benefit calculus, they can be deterred. Thus, increasing the costs of action by the deterring side is important. The party which deters should hold something at risks which the adversary values. Deterrence by denial is relatively simple; deterrence by punishment is more difficult; here the analytical literature can cite only few successes. Deterrence can be a form of prevention in counterterrorism.

Keywords: counterterrorism, counterinsurgency, deterrence, doctrine, insurgency, prevention, strategy, terrorism
After the end of the Cold War, Counter Insurgency (COIN) operations and counterterrorism operations became the main focus of some of the armed forces of the West. With the threat of large-scale conventional and nuclear war seemingly belonging to the past, major Western powers prepared to fight “wars of choice” in distant places against insurgents, using unconventional war fighting tactics, exploiting weaknesses of the adversary.

Rebel forces seek to break the ties between the incumbent regime and the population. To achieve this goal, they apply asymmetric warfare tactics such as “hit-and-run” attacks and acts of urban terrorism. Western armed forces soon discovered that they were not prepared for this kind of warfare. Reaching back to the overseas battles France and Great Britain fought in their colonies in the 19th and first half of the 20th centuries, and using the lessons learned from the Vietnam war and other traumatic experiences, the military started drafting new COIN doctrines for dealing with complex contingencies. Military leaders relearned how to fight wars against insurgents, albeit with mixed success.

The first part of this chapter provides an overview of the making of contemporary military COIN doctrine. As COIN is population centric, COIN doctrine may provide important lessons for any situation where authorities fight terrorists which have roots in sizeable segments of society, as is the case with jihadists. To the knowledge of this author, little research has been done on the application of COIN doctrines to domestic counterterrorism operations.

The second part of this chapter deals with deterrence and prevention and seeks to apply the lessons and principles learned by some Western countries which were affected by terrorist attacks. It is argued that deterrence is firmly embedded in modern COIN doctrine and that such a doctrine can provide important clues and offer “lessons learned” for counterterrorism operations in, and by, Western states.

It is important to remember that COIN was designed for dealing with an insurgency, not for preventing it. From a military perspective, prevention requires deterrence. Thomas Schelling defined deterrence as “persuading a potential enemy that he should in his own interest avoid certain courses of activities.” This requires persuading an actor that the costs of taking action outweigh the possible benefits. A cost-benefit calculus is at the heart of any deterrence strategy. This presupposes, however, that terrorists, like states, are rational actors.

Military Doctrine

Doctrine differs from strategy. Strategy is defined as a set of ideas implemented by military organizations to pursue desired goals. The Oxford Dictionary defines strategy in non-military terms as a plan of action designed to achieve a long-term or overall aim. Strategy is considered to be the single most important factor for success. Without a clear strategy and a doctrine, any military operation is likely to fail.

Without a strategy, political, and consequently military, objectives cannot be defined and without doctrine the military does not know how to employ armed forces under its command. Doctrine spells out the fundamental principles that guide military forces as they pursue national security objectives. Many of its principles are rooted in the past and have been adapted over time to meet new needs. Without a sound doctrine and a correct strategy armed forces cannot be effective. The same holds true for national counter terrorist agencies and the units under their command. To be effective, they also need the right doctrine and the right strategy.

The military of the United States makes a clear distinction between COIN and counterterrorism. The US Army’s Joint Publication 3-24 (2009, updated in 2018) deals with counterinsurgency operations (COIN doctrine), whilst Joint Publication 3-26 (2014) addresses counterterrorism (counterterrorism doctrine). The doctrine defines insurgency as the organized used of subversion and violence to seize, nullify, or challenge political control of a region. This doctrine views insurgency as a form of intrastate conflict and COIN as a method to counter it. Counterterrorism doctrine defines terrorism as the unlawful use of violence or the threat of
violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political. Furthermore, the manual considers terrorism as a tool of irregular warfare while counterterrorism activities and operations are taken to neutralize terrorists, their organizations and networks.\(^4\)

Most American doctrines are coextensive with the doctrines of other NATO member states. However, while NATO published an Allied Joint Publication on counterinsurgency (NATO counterterrorism doctrine AJP 3.4.4) in July 2016, it lacks a dedicated counterterrorism doctrine.

There two schools of thought on COIN and counterterrorism. The first school of thought believes that terrorists are clearly identifiable individuals and small groups or cells that are not supported by large parts of the population. Terrorists without deep roots in society - such as Anders Breivik, who was responsible for the Oslo and Utøya attacks (Norway, 2011), Brenton Tarrant, who killed 51 people in the Christchurch mosque attacks (New Zealand, 2019) and other right wing extremists - may enjoy some sympathy among right-wing fringes within society, but lack broader public support. Doctrine explains how those individuals or cells should be neutralized when separated from the population. The F3EAD process is the heart of contemporary US counterterrorism doctrine. F3EAD stands for find, fix, finish, exploit, analyze and disseminate. This process explains how a counterterrorism operation is to be planned and executed. It is aimed at analyzing the situation and spot terrorists through intelligence (find); establish the location (fix); capturing or killing them (finish); questioning and screening those present at the target site and collect material on the site (exploit); and place this information (analyze) into the greater body of knowledge about terrorist organizations (disseminate).\(^5\)

The second school of thought sees counterterrorism as part of counterinsurgency operations. Whereas counterterrorism doctrine sees terrorists as clearly identifiable individuals, cells or groups that can be identified and hunted down, COIN is focusing more on their environment - a population centric approach. COIN doctrine considers terrorists as being a part of a broader social movement. COIN doctrine explains how insurgents are embedded in society and how they try to find legitimacy from deeply rooted socio-economic and political grievances in society. In this school of thought, insurgencies are viewed as protracted politico-military struggles aimed at undermining the legitimacy of a government or an occupying power.\(^6\) As a consequence, the operational method of COIN usually takes the form of “shape, clear, hold, build.” Shape sets the conditions for the operation by either reassuring the population or by deterring and dissuading it; clear aims to remove or eliminate guerrilla forces from an assigned area; hold requires the friendly forces to secure the population and eliminate remaining fighters; build is aimed at restoring services and civil control, providing support to the rebuilding of infrastructure and economic development.\(^7\)

The distinction between the two approaches goes back to the 1970s when terrorist groups, such as the Red Brigades in Italy and the Red Army Faction (RAF) in the German Federal Republic, were considered isolated cells lacking broad public appeal and support. The supporters of this school of thought argue that terrorist organizations cannot be disrupted through COIN-techniques and, conversely, that insurgents are resilient to counterterrorism-techniques.\(^8\) As these are two models of conflict, the main argument is that insurgents and terrorists cannot be confronted with a one-size-fits-all approach. However, COIN and counterterrorism can be mutually reinforcing. When insurgents are separated from the populace, they can be hunted down by units using counterterrorism-techniques.

Some theorists argue that a “neo-classical framework” underpins COIN doctrine. COIN doctrine has, as mentioned above, its roots in colonial and Cold War era insurgencies. As Matthew Cancian has argued, the COIN doctrine “frames insurgency as a contest between insurgents and governments over an undecided population, a contest whose outcome is principally determined by the relative capability of each side to govern people.”\(^9\) Consequently,
the struggle for the “hearts and minds” defines the outcome. Winning the “hearts and minds” should deny terrorists from achieving their political objectives. A successful “hearts and minds” campaign can also contribute to deterrence.

Unsurprisingly, American COIN doctrine mentions the lack of state capacity as an important reason for lack of popular support. This will have detrimental effects in revolutionary wars where the grievances articulated by rebel leaders are shared by larger segments of the population often independent of their particular religion, beliefs or loyalties. However, this is not necessarily the case in ethnic or tribal conflicts where the government is often seen as illegitimate. The strengthening of the state from the outside can then be seen as a violent act which runs against the interests of a particular minority group. In a federally organized state such as Iraq, the Kurdish minority will not accept a strengthening of the federal government at the expense of its relative autonomy. This raises the question whether COIN is applicable for ethnic or tribal conflict as well.

Where a distinction between insurgency and terrorism cannot be made, the difference between COIN and counterterrorism becomes blurred. The Taliban movement’s campaign of violence in Afghanistan clearly is an insurgency. It is part of a broader Pashtun movement and deeply rooted in a large segment of the population. Its struggle is politically motivated and its strategic objectives are clear: remove the illegal occupying force from Afghanistan’s soil and topple what they consider an illegitimate government. In achieving its objectives, Taliban insurgents fight an unconventional or irregular war that includes terrorist tactics.

What about terrorist organizations such as ISIS and Al-Qaeda? They also fight against regimes they consider illegal. Both ISIS and Al Qaeda enjoy support among parts of the populations in the Muslim world. After the US intervention in Afghanistan in 2001, Al-Qaeda fled to the tribal areas in western Pakistan where it was hiding among sympathetic tribes. In Iraq and Syria, ISIS was initially supported by local Sunni tribes and anti-regime groups. In Europe, small parts of local immigrant diaspora populations support Muslim extremist and terrorists as well. In the case of religiously inspired terrorism, the distinction between terrorist groups and insurgency quickly became blurred. But the same could also be said about Catholic separatists in Northern Ireland or Basque nationalists in Spain. There is considerable sympathy and support among the population for terrorist organizations such as Islamic State of Iraq and Syria (ISIS), Al-Qaeda and various separatist movements. The same holds true for their sympathizers in Western diasporas. Regarding Al-Qaeda, the American polling organization Pew concluded in 2013 that

“a median of 57% across the 11 Muslim publics surveyed holds an unfavorable view of Al Qaeda. This includes strong majorities of Muslims in Lebanon (96%), Jordan (81%), Turkey (73%), and Egypt (69%). More than half of Muslims in Nigeria, Senegal, Tunisia, Indonesia, and the Palestinian territories also view Al Qaeda negatively. In Pakistan and Malaysia, Muslim views of Al Qaeda are on balance unfavorable, but many offer no opinion.”

With hundreds of millions of Muslims living in these countries, those not holding unfavourable views still amount to tens of millions of people. For this reason, Al Qaeda might believe that it could still win the battle for “hearts and minds”.

For ISIS, support was generally less. This is partly the result of the many atrocities perpetrated by the self-proclaimed Islamic State. The Doha-based Arab Center for Research and Policy Studies found that 85% of Arabs hold, to varying degrees, negative views of ISIS. This compares to only 11% of the Arab public whose views towards the group were either “Positive” or “Positive to some extent.” Nevertheless, the remaining 11 percent translates into millions of people which could serve as a sanctuary or support base.
The objective of both ISIS and Al Qaeda is a worldwide insurgency against “corrupt” leaders in the Islamic world and the withdrawal of Western support for them. The Doha Report revealed that important reasons for backing ISIS include its willingness to challenge the West and its opposition to Iran and the Syrian and Iraqi regimes. In other words, despite negative views about its methods, the objectives of ISIS have the sympathy of a sizable minority of Arabic populations. Winning more support looked, for a while, not like an impossible task as long the Islamic State had control over a large territory straddling Syria and Iraq.

In May 2019, a video was released showing ISIS leaders Abu Bakr al-Baghdadi announcing wider geographical ambitions following the territorial losses in Syria and Iraq. Allegiance for ISIS has already been given by jihadists in Afghanistan, Burkina Faso, Mali, Nigeria, Sri Lanka and other parts of the Islamic world. This continued loyalty demonstrates that despite the defeat of the Islamic “State” in the Middle East, the brand still possesses great attraction beyond the Arab region. ISIS’s apocalyptic ideology and sectarian attacks on unbelievers such as Shiites and Christians did not disappear with the end of ISIS’s “formal state.” At the same time, the survival of its ideology and the organization of a worldwide network of franchises and cells mark the failure of the US-led coalition to destroy the organization. Even with the defeat of its “Islamic State” in Syria and Iraq, ISIS is not a small group of dedicated, clearly identifiable terrorists, but a broad-based terrorist organization with roots in the Sunni ummah around the world. To underscore its new strategy, ISIS claimed responsibility for the Easter bombings in Sri Lanka in 2019, which killed more than 320 people. ISIS claimed the bombers in Sri Lanka targeted citizens of the US-led coalition fighting ISIS and referred to Easter as an “infidel holiday.”

The conceptual challenge is whether the defeat of ISIS and Al Qaeda requires COIN or counterterrorism tactics or a combination of both. As has been argued above, a distinction is made between an insurgency and isolated terrorism. Isolated terrorists are lone wolves or isolated cells and small groups. Unfortunately, there is a tendency to consider “terrorists” as derailed individuals while ignoring the fact that those individual terrorists or small terrorist groups may reflect grievances among larger parts of the population. In such cases, even an “isolated” terrorist may gain considerable support from a sympathetic segment of the populace.

In cases of foreign intervention, this ideological and operational support base may even grow bigger if the intervening force is considered an adversary. The support base of isolated terrorists in the West may also grow stronger if interventions, e.g. in the Islamic world, are considered hostile actions. This is one of the contributing factors for jihadism in the West. Consequently, the distinction between insurgency and terrorism is by no means always clear. Insurgency and terrorism are both political struggles for which the position of the population is crucial. How COIN and counterterrorism works out on the population has always been considered key to the success of any operation against insurgents and terrorists. If policy makers in the West can agree that terrorists indeed reflect deeper grievances among the population, COIN doctrine might provide some very important lessons for counterterrorism operations. Without the acknowledgment that a clear distinction between jihadists and insurgents cannot be made, a counterterrorism operation is likely to be based on the wrong strategy. Therefore, COIN and counterterrorism doctrine provide important lessons for combatting terrorism also in the West.

Another question is whether insurgents and terrorists will be deterred by the prospect of foreign intervention. Effective deterrence will require effective COIN and counterterrorism operations. However, in this regard, the track record of Western powers is bad. At the same time, the negative experience with foreign interventions can provide important Lessons Learned for domestic counterterrorism.
Not the Right War

Why is combatting insurgencies so difficult? One explanation is that the armed forces of liberal democracies have been traditionally trained and equipped for conventional interstate wars. The main preoccupation is relatively static defenses with large units, i.e. divisions and army corps. Those units with their focus on heavy firepower, technology, maneuverability and a state adversary with similar capabilities are inadequate for COIN operations.

After the end of the Cold War Western armed forces were deployed in complex contingencies, defined as “internal conflicts with large-scale displacements of people, mass famine, and fragile or failing economic, political, and social institutions.”13 Years of conflict and persecution, often fueled by selfish motives of political entrepreneurs, could cause a breakdown of government and chronic insecurity. Violent eruptions usually follow deliberate efforts of determined leaders in response to corruption, discrimination, economic failure, mal-administration, repression and poor economic conditions.

Complex contingencies tend to unfold in less developed parts of the world. Only very rarely do these involve regular armies on both sides. More often than not, regular forces on one side fight guerrilla forces, terrorists, and armed civilians on the other.14 In those circumstances, low-intensity war will replace high-intensity interstate warfare almost completely, because opponents are likely to fight in an asymmetrical way.15 However, “low-intensity” can be misleading. It suggests a low level of violence and limited numbers of casualties. But even in low-intensity conflicts, thousands, sometimes even million of civilians, can and have been displaced with many of them dying from hunger, diseases and cold.

Actually, this is nothing new. In 1898, in Lockhart’s Advance Through Tirah, Captain L.J. Shadwell wrote about “savage warfare”, also known as colonial or non-European warfare “that differed from that of civilized people.”16 Many areas in the world have not changed much since Shadwell’s description:

“A frontier tribesman can live for days on the grain he carries with him, and other savages on a few dates; consequently, no necessity exists for them to cover a line of communications. So nimble of foot, too, are they in their grass shoes, and so conversant with every goat-track in their mountains that they can retreat in any direction. This extraordinary mobility enables them to attack from any direction quite unexpectedly, and to disperse and disappear as rapidly as they came. For this reason, the rear of a European force is as much exposed to attack as its front or flanks.”

For example, in Afghanistan, the biggest change was that army boots and Nike sport shoes replaced Shadwell’s grass shoes. Local fighters of the Taliban and al-Qaeda generally possess only a limited number of advanced weapons, such as Stinger anti-aircraft missiles, which were acquired during the 1980s when the U.S. considered the mujahedeen to be freedom fighters who deserved support in their struggle against the Soviet occupation. Today’s basic weapons platform is the Toyota pick-up truck, which carries fighters armed with guns; in mountainous regions horses and mules are still an important mode of transportation. The main innovation is the use of the Internet, cell phones and satellite communication for command-and-control purposes and social media for both winning the “hearts and minds” of sectors of the Muslim world and for deterring adversaries. The appalling videos of beheadings and other atrocities broadcasted by ISIS were, inter alia, meant to deter the adversary from entering a war against ISIS.

One might argue that ISIS succeeded to deter a ground war by the US lead coalition. Western leaders had already concluded that public - and consequently political - support would plummet if soldiers were to be butchered in front of video cameras. This was a hard lesson learned during the “battle of Mogadishu” at the end of which several US casualties were
dragged behind cars through the streets of the Somali capital in 1993 by local fighters in front of rolling cameras. This highly publicized incident led to the conclusion by policy-makers in Washington that the operation had failed and that American troops should be withdrawn. Since the “battle of Mogadishu”, the preferred tactic of Western forces was the use of air power while conducting ground operations with the help of local proxies. This was the preferred choice during the Kosovo war (1999) as well and remained so in the war against ISIS where Kurdish fighters acted as proxies.

**Insurgent Strategies**

Revolutionary warfare is an insurgent strategy aimed at removing an “illegitimate government.” Mao Zedong provided the first coherent theory of revolutionary struggle, using a mix of unconventional and conventional warfare techniques. He had a clear idea of the strengths and weaknesses of unconventional warfare. Therefore, his ideas are still important in understanding this kind of warfare. Mao wrote two books about the subject: *Guerrilla Warfare* (1937) and *Strategic Problems in the Anti-Japanese Guerrilla War* (1938) in which he maintained that the struggle is primarily a political one, rather than only military. The notion of a political struggle helps understanding both contemporary counter insurgency operations and domestic counterterrorist operations. Ignoring the political dimension can have serious consequences and lead to the choice of a wrong strategy and doctrine. Mao Zedong outlined a seven-step strategy that any revolutionary strategy must follow:

1. Arousing and organizing the people;
2. Achieving internal unification politically;
3. Establishing bases;
4. Equipping forces;
5. Recovering national strength;
6. Destroying enemy’s national strength;
7. Regaining lost territories.

Subsequently, Mao identified his famous three stages of insurgency:

- The first stage is one of the enemy’s strategic offensive and our strategic defensive that would require guerrilla warfare.
- The second stage is one of the enemy’s strategic defensive and our preparation of the counter-offensive.
- The third stage is one of our strategic counter-offensive and the enemy’s strategic retreat. This would require conventional warfare.\(^{17}\)

Mao’s strategy has been described as *Protracted Popular War*. This strategy was developed to gain control over rural areas where government control was weak or absent. It was based on the assumption that the revolutionary cause would attract an ever-increasing number of supporters. Insurgents would then establish secure base areas, build parallel political and military structures and gradually expand their zones of influence. The strategy involves a mix of terrorism, guerrilla tactics, and political agitation. The political outreach, aimed at poor peasants, was the most important. Good social work was used to gain the support of the willing part of the population. Terror and intimidation was used to “gain support” of the unwilling part of the population. The local population was used for recruitment, logistics, and shelter. In its initial stages, rural insurgencies rely on small bands of men. Usually they carry out small-scale operations in remote areas, engaging in ambushes, sabotage, acts of terrorism, and assassinations. As the movement becomes more successful, its objectives become more ambitious, so that larger formations can be called into existence. The transformation of
irregular guerrilla forces into a regular army is, in Mao’s thinking, considered necessary to gain final victory.

This is illustrated by the Maoist insurgency in Nepal and the establishment of the Caliphate in Syria and Iraq. By the end of 2002, Marxist rebels in Nepal were ready to move into the final stage of the insurgency. They launched a strategic offensive, with some 3,000-4,000 regular troops and some 10,000-15,000 men and women organized in local militias. Next to Mao’s Chinese Communist insurgency, this is one of the very few examples of a rebel group that managed to transform itself into a conventional armed force. The Nepalese Maoists won the war, not because they were superior in numbers, but because the Royal Nepalese Army was demotivated, lacked combat experience, was short of necessary logistics, and had no effective counterinsurgency strategy based on good intelligence.

ISIS is the most recent major example of a movement following in Mao’s military footsteps. ISIS considered the governments of Iraq and Syria as illegitimate and believed that both countries should be part of a newly established Caliphate. However, ISIS’s revolutionary struggle failed in the end because the anti-ISIS coalition carried out relentless bombardments on ISIS positions. The ground war was fought by skilled proxies such as the Kurds. Consequently, ISIS was unable to implement the third stage of Mao’s revolutionary struggle. The inability to conduct conventional warfare is an important explanation for ISIS’s failure.

Mao’s strategy is only one of several strategic recipes for insurgencies. For achieving their objectives, insurgents have also turned to the following strategies:

- Conspiratorial strategy: This strategy is designed for an urban environment. Small cells of leaders try to generate uprisings by means of armed action, and attempt to get media coverage. The strategy aims to seize key points and decapitate the governing regime.
- Military strategy: In this strategy, political action is secondary to military action. The assumption is that the population will choose the winning side. The strategy focuses on discrediting the government’s security forces. Initially, the insurgents are likely to apply guerrilla warfare techniques with small mobile forces. As the movement is getting more successful and more men are available, conventional warfare techniques may be applied.
- Urban insurgency: This strategy involves applying tactics of organized crime and terrorism in a systematic manner. Insurgents try to disrupt city life through creating terror, ethnic cleansing, assassination of public figures, establishing no-go areas, and mounting attacks on public services. The aim is to undermine the credibility and the morale of authorities. For that reason, demonstrations can also be engineered. Insurgents will seek media coverage to generate panic. Violence is the catalyst for political change, e.g. by forcing a repressive military response that in turn will alienate the masses and move them to revolt. In contrast to the Popular War, the insurgents cannot use the population for recruitment and logistics, but he will use the population as shelter. Again, media coverage is crucial.
- Isolated terrorism: This strategy seeks to undermine society and government through assassinations, kidnappings, hijackings, sabotage, bombings, raids, and attacks on public facilities. This form of terrorism is considered a local or tactical challenge, which should be handled by the internal security forces, the police, and the intelligence communities.

In all cases, the struggle is political with the population at its center. The key challenge is how to get the support of the population. The insurgents’ constructive activities involve the formation of cadres for training, the creation and development of areas for subversive activities, the organization of alternative police and military units to take over internal and external
security tasks, and the creation of an administrative machinery to raise taxes and replace the
government’s bureaucracy.

Insurgents will also seek extensive media coverage. First, they can use their own radio and
TV stations and the Internet to promote their cause. Both Al-Qaeda and ISIS continue to make
extensive use of the media, e.g. by posting videotapes. Second, they try to win the heart of the
population. In some cases, insurgents have become popular because they provided a
rudimentary welfare system, including health care and education. In the Islamic world,
fundamentalist groups seek to develop a social and cultural infrastructure to build an Islamic
civil society and fill a vacuum that their countries’ governments have failed to fill. During the
1990s in Egypt, Jordan, the Palestinian territories, Afghanistan, and Pakistan, radical
movements sought to provide health care, education, and welfare for the poor. Radical
movements such as Hamas and Al-Qaeda use nongovernmental organizations (NGO)
extensively as fronts for such purposes. After the 1992 earthquake in Cairo, organizations like
the Muslim Brotherhood were on the streets within hours, whereas the Egyptian government’s
own relief efforts lagged behind. Bin Laden was popular because of his “good works” in parts
of the Islamic world, especially in Sudan and Afghanistan. Quranic study centers have become
one of the important sources for recruiting new members for extremist movements. These
types of activities have successfully undermined the legitimacy of governments, while gaining
the support of segments of the civilian societies.

Destructive activities are usually aimed at undermining the political elite’s authority and
power base, including the internal security forces, the police, and the armed forces. By creating
a climate of insecurity, the population is likely to lose faith in the authorities. Intimidation,
sabotage, terrorism, information warfare, and guerrilla attacks are the most likely tactics
employed. Insurgents will try to balance their political aims and the means of achieving them.
If the means and ends mismatch, insurgents may lose popular support. In 2005, Al-Qaeda’s
number two, Zawahiri, accused Abu Musab al-Zarqawi Al Qaeda’s leaders in the Levant of
alienating Iraq’s Sunni masses through their brutal campaign of beheadings and bombings.
Years later, due to excessive violence, ISIS also lost much of its initial support in the battle for
the people’s “hearts and minds.”

The Foundations of COIN

How to fight insurgents has been a problem for colonial powers for centuries. Great Britain,
France and the Netherlands were among the major colonial powers which fought bitter wars
against those who considered them as occupying forces. In the 1960s, the US learned similar
hard lessons. Yet the Vietnam War (1965-1973) was considered an aberration and the lessons
learned were soon forgotten. The disastrous performance of U.S. troops contributed to the
neglect of unconventional warfare. As a result, a second, though minor disaster in Somalia
(1994) followed. Preoccupation with conventional wars is equally strong in other armies.
Soviet forces performed disastrously in Afghanistan (1979-1989).

The same happened to the Netherlands. With the loss of Indonesia in the late 1940s, the
Dutch lost not only their experience in waging this type of war, but also their mental acumen
for such warfare. Nevertheless, in 2001, when drafting a new field manual on
counterinsurgency warfare, the Dutch army staff also consulted the old manuals of General
Johannes van Heutz (1851 – 1924). In the Netherlands Indies (present-day Indonesia), van
Heutsz had reorganized his conventional ground forces to confront insurgents, creating small
units of a dozen men to carry out search-and-destroy operations. No distinction was made
between combatants and non-combatants in those operations. The Dutch troops burned down
entire villages in order to eliminate fighters’ bases. Today, that type of counterinsurgency
operations would be categorized as war crimes.
In addition to Van Heutsz’s manuals, in drafting the new manual, the Dutch army staff also used the British counterinsurgency manual, which is one the most detailed for this type of warfare. Of the former colonial powers, the British – and to some extent the French - have not given up their colonial military skills and the mindset to carry out counterinsurgency operations. Especially, the counterinsurgencies in the Dhofar province in Oman (1965-1975) and “The Troubles” in Northern Ireland (1969-1998) have given the British first-hand experience. In Dhofar, strategic interests were at stake because Oman’s leaders could control the vital oil route of the Strait of Hormuz. The Dhofar campaign was a classical, rural counterinsurgency campaign, while the one in Northern Ireland was a mix of rural and urban fighting. To this day, the most elaborate COIN doctrine remains the one developed by the British military.

An important Lesson Learned has been that unconventional warfare is first of all a method of achieving asymmetry. Asymmetry is a key concept for confronting the adversary not on his own terms. It is often the tactic of the weak. At the strategic level, the opponent using asymmetrical tactics exploits the fears of civilian population, thereby undermining the government, compromising its alliances, and affecting its economy. To achieve this, the opponent uses unconventional warfare techniques at the tactical level to change the course of action in order to prevent the opponent from achieving political objectives. The tactics of unconventional warfare include guerrilla ambushes, hit-and-run attacks, sabotage, terrorism, and psychological warfare. Usually, rebels, terrorists and criminals with small, but well-organized forces or militias tend to adopt such tactics.

In unconventional warfare it is only through the physical control of an area or isolation of the opponent that military objectives can be met. This requires the use of small units. Advanced technology plays a supporting role at best. In conventional warfare, those operating at the strategic level provide the overall direction; those on the operational level are concerned with armies and army corps fighting campaigns; those operating on the tactical level are concerned with divisions and brigades fighting battles; those on the technical level deal with small units and the effects of weapon systems.

In unconventional warfare two levels are most important: the strategic level for overall direction and the technical level for the actual war fighting. The strategic level also deals with political influence operations and diplomatic actions. The operational and tactical levels oversee the operation in the target area and can play a supporting role, e.g. to provide air support for soldiers on the ground. Most importantly, the operational level will oversee the “hearts and minds” campaign, including psychological operations, carried out at the tactical level. Thus, in conventional warfare, doctrine deals with the interaction between the various levels of war. In unconventional warfare, the different levels fight different “battles.” The different roles of the levels in conventional and unconventional warfare make it extremely difficult for commanders to conduct both types of operations simultaneously.

In unconventional warfare, skills are important factors for success. Because the skills of Western forces are traditionally limited to a small part of the total war fighting spectrum, the chances of success are limited when facing irregular forces. This demands capabilities in the field of counter-guerrilla warfare, which most Western powers have not been trained for.

As conventional warfare in open terrain is the preferred form of combat for modern Western military forces, insurgents and terrorists seek to avoid open terrain. They prefer to confront the adversary in cities and mountains. This creates a fundamental problem for Western political and military leaders. Military history suggests that it is extremely difficult for modern forces to use their technological advantages in a “complex terrain.” Mountains are no-go areas for tanks and armored vehicles. They can only be used to block roads and to provide fire support. The actual fighting requires small units that carry out search-and-destroy missions. Troops hunt down the adversary and neutralize the enemy in close combat. They can call in air
power, but in practice there is a shortage of rewarding targets for bombing, because air power is unlikely to find and destroy small bands of fighters.

As a result of the wars in Yugoslavia, Afghanistan and Iraq, a renewed focus on unconventional warfare has emerged as a priority in US military thinking. But only the 2003 version of the U.S. field manual Operations described the basic tenets of counterinsurgency operations in detail. The manual stressed that counterinsurgency was essentially a political task aimed at neutralizing the adversary. While there was no indication that the US Army embraced the concept with enthusiasm, the ongoing struggle with insurgents in Afghanistan and Iraq forced its leadership to adopt an interim counterinsurgency manual.\textsuperscript{20}

Given the poor record in counterinsurgency operations, major powers often seek a solution in fighting wars by proxy. Local fighters usually have a greater understanding of both the terrain and the adversary. Moreover, they are usually highly motivated, because they have an existential cause to fight for. In Mindanao, in the Philippines, US Special Operations Forces conducted joint operations with the Filipinos against the Abu Sayyaf Group, which was suspected of having close links with Al Qaeda. Some 600 US Special Operations Forces formed a joint team with the armed forces of the Philippines.

However, local fighters can be unreliable, because they might consider outside powers as a means to achieve their own ends. This happened during Operation Allied Force, when the Kosovo Liberation Army (KLA) considered NATO as its own air force. The KLA was convinced that NATO would support its cause, i.e. an independent Kosovo. If there is a mismatch between expectations and real interests, local fighters may turn against the intervener. For this reason, Western armed forces may at times have no other choice than to fight unconventional wars themselves.

Later, in Iraq and Syria, the Americans fought again proxy wars against ISIS. Kurds fought the ground war while the US-led coalition provided intelligence and air power. An important reason for proxy wars is the aversion for causing casualties among friendly state allies and the fear of committing war crimes or major collateral damage. However, breaches of the laws of war are an inherent risk of all COIN or counterterrorism operations.

There are two techniques for direct action to physically control an area: attrition or brute force. Straightforward attrition is based on absolute repression and destruction of the adversary. Firepower is the key to success. Mobility is primarily used to maneuver firepower into favorable positions. Relentless bombings and attacks with heavy weapons systems such as tanks and artillery and the systematic destruction of buildings by bulldozing or demolition are common techniques. The advantage is that it can be done with limited friendly losses; the disadvantage is the high level of destruction. The Russians leveled Grozny during the first Chechen War; in 1988 Saddam Hussein used chemical weapons against Kurds in Halabja; in 2002, Israeli forces destroyed parts of Jenin in an attempt to stop suicide attacks on Israel’s soil; in 2004 the American military destroyed much of Fallujah in an attempt to crush the Iraqi insurgency. The US-led coalition came close to attrition during the battle of Mosul (2016–2017) to clear the city of thousands of ISIS fighters. Iraqi government forces and the Kurds carried out the ground operations while the US-led coalition forces provided logistical and air support, intelligence, and advice.\textsuperscript{21}

Unsurprisingly, in all of these cases, military leaders were accused of barbarism and war crimes. In Mosul, the most widely covered incident was a March 17, 2017, coalition air strike on homes in the Jadidia neighborhood whereby at least 105 civilians were killed. A report by the NGO Airwars concluded that the “urban battles show a close correlation between intensity of munitions use and population density, and negative outcomes for civilians” and that the US-led coalition was responsible for civilian death tolls “not seen since Vietnam” in the fight against ISIS.\textsuperscript{22}

In all of the conflicts just mentioned the intervener was in the end unable to win the “hearts and minds” of the population. Attrition is an inappropriate strategy for liberal democracies.
Moreover, the record of success for an “attrition only” strategy is generally poor. Insurgents will flee the city, regroup and continue the fight. Once more, ISIS is a case in point. After having lost the “Caliphate,” its leader, al-Baghdadi, announce a new phase in the struggle against unbelievers and illegitimate regimes, based on IS franchises and sympathizers all over the world. Nevertheless, armies trained and organized for conventional warfare may consider attrition as a tactic of last resort as was the case in the fight against ISIS. This, however, runs the risk of further strengthening the remaining fighters’ resolve. Moreover, heavy civilian casualties will increase hatred among the population and turn people against the intervening force or against local authorities held responsible.

**Maneuver**

A counterinsurgency campaign is maneuver warfare in its most basic form. The Iraqi government forces and the Kurds in Mosul practiced this type of operation. Direct action to gain control over an area involved cutting off logistics (isolation), engaging in cordonning and search-and-destroy operations. A well-tested approach in combating insurgents is the *inside out* method of expanding secured areas. The aim is to consolidate areas. First, a bridgehead inside the area is established. Second, friendly and local loyal forces are used to secure the surrounding area in order to release regular mobile troops to secure the next area. Securing adjacent areas can be done with specialized troops, such as air-mobile and air-maneuverable troops as well as Special Operations Forces. Combating insurgents usually requires deploying small patrols into the terrain that insurgents consider their own. Surprise, speed and simultaneous actions are used to overwhelm the adversary, bringing about a collapse of will and ultimately helping to create conditions for a political solution. Nevertheless, force should be applied in a selective and controlled manner. Limiting collateral damage is extremely important in order to spare the lives of non-combatants.

Typical operations are *search and destroy*, and *cordon and search*. Both operations are difficult to execute. First, the search part is usually a lengthy affair. Second, cordon operations are difficult because closing a cordon quickly and effectively is nearly impossible. Maneuver warfare theory assumes that shattering the adversary’s moral and physical cohesion is more effective than achieving his destruction. Consequently, the strategy focuses on people and ideas rather than military victory.

Therefore, minimal use of force works best, because the insurgents will attempt to demonize intervening forces or local authorities when these use excessive force. In addition, intense media coverage could also undermine the effectiveness of the operations in the case of excessive force use. Media coverage can also undermine support for the operation if there is a widespread feeling that international law is not being obeyed or injustice is done. In other words, excessive force runs the risk of losing the support of the people.

Operations in urban areas pose the greatest challenge for modern armed forces. As Ralph Peters put it: “The future of warfare lies in the streets, high-rise buildings, industrial parks, and the sprawl of houses, and shelters that form the broken cities of the world.” In most parts of the world, but particularly in Europe, urban and industrial areas continue to grow in number and size. More than half of the world’s population lives in cities. Almost 70 percent will be living in urban areas by 2050. The biggest cities already have populations in excess of 30 million.

Consequently, most political and social unrest is likely to occur in urban areas. Urban warfare can be extraordinarily destructive, especially if a strategy of attrition is applied. Fighting in urban environments also places many restrictions on allied operational commanders, as they are responsible for protecting civilians and their property. Indeed, one of the most notable differences with open terrain is the great number of non-combatants in the combat zone. Thus, limiting collateral damage is crucial. Yet at the same time, limiting
collateral damage is extremely difficult, because urban warfare usually requires cordon operations, followed by systematic house-to-house search-and-destroy operations. Fighting in cities requires small groups of dismounted soldiers engaging in close combat. The rifle and the machine gun are the most common weapon in urban warfare.

As the liberation of Mosul from ISIS has demonstrated, close air support with fixed-wing aircraft in an urban environment is challenging. Targets are difficult to locate and identify, and enemy and friendly forces tend to be intermingled. Furthermore, low-flying aircrafts are vulnerable to shoulder-fired surface-to-air missiles and even to rocket-propelled grenades. Aircraft and drones will be useful for surveillance and reconnaissance, communication and liaison tasks, the insertion of special forces and troop lifts as well as for psychological operations (dropping leaflets, broadcasting from airborne radio and TV stations), close air support, and interdiction.

Small-scale urban operations involve traditional *policing operations* to prevent the outbreak of violence. Raids can have different objectives, for example evacuating nationals, rescuing hostages, or seizing key facilities such as airfields. The key to success is surprise and the use of overwhelming force. The insertion and extraction of forces is the hardest part in such operations. Good intelligence is the key to success.

Instead of conducting a direct assault on a city, the attacker should first establish a loose cordon around the city and control the surrounding countryside. This was the first phase of the US-led siege of Baghdad in 2003. American troops blocked all avenues, controlled the airfields in and around the capital, took control of the sources of electrical power, water, and food, and carried out air strikes against leadership targets in the city. This technique was also applied after the withdrawal from Fallujah, Iraq, in March 2004.

But to take a city, units have to enter it. There are three different tactical concepts for large scale urban operations.

- **Urban penetration:** This tactic is designed to quickly maneuver to the target area and establish control in a dispersed and non-contiguous area.
- **Urban thrust:** This tactic is focused on achieving an assault against the adversary on a narrow axis of attack. As this attack is occurring, the axis of advance is defended in order to hold the flank against potential enemy attacks.
- **Urban swamp:** This is similar to the tactic used by police forces responding to an emergency that requires backup. The concept requires numerous small teams operating in a dispersed, non-contiguous fashion.

Of crucial importance is the "hearts and minds" campaign, which seeks to win the support of the population, accompanied by psychological as well as information operations. The objective is to separate enemy fighters from their base. Such an effort, often combining several approaches, including humanitarian aid and propaganda, must be made in parallel with diplomatic measures and military operations. From 1985 until 2000, Israel carried out a counterinsurgency campaign in Southern Lebanon, while at the same time providing assistance to the Lebanese population, including projects to rebuild the infrastructure and programs to provide health care. In Afghanistan, during Operation Enduring Freedom, food was used as a weapon. C-17 air lifters dropped tens of thousands of packets of food and medical supplies in Afghanistan in 2001. Each package contained the message that it was a gift from the people of the United States of America. In addition to food rations, U.S. aircraft dropped leaflets and small transistor radios to enable Afghans to receive Washington’s message. It was part of a dual strategy of diminishing the Taliban regime’s hold over the population and gain popular support.
Planning an Operation

The planning of a counterinsurgency operation, requires first an analysis of the type of conflict, its implications, and the method to stop, neutralize or reverse actions of the opponent. To achieve the desired end state, clear political objectives must be defined. During the campaign, civilian political authorities will keep overall responsibility, while delegating implementation to military authorities. The way to rein in rebels, terrorists, and gangs is to separate them from their bases, either physically or politically. This is done by denying them information, logistics, recruits, funding, safe havens, and popular support through physical separation and “hearts and minds” campaigns aimed at winning the support of the local populace. The latter is important because the strategic center of gravity is the support of the mass of the population. Consequently, in contrast to conventional warfare, unconventional warfare seeks to avoid attacking the center of gravity. Military victories will therefore never be sudden and spectacular. Rather, victory will be achieved by a sequence of small successes.

The aim of COIN is to secure the population and to neutralize the insurgents. This requires the commander to pursue four military objectives that contribute to the successful attainment of political goals:

1. secure the population;
2. isolate the insurgents from their support;
3. neutralize the insurgents’ subversive strategy and armed organization; and
4. support other organizations in planning to create unity of effort.26

The objective is to deny insurgents and terrorists from achieving their political objectives and neutralizing them and their support systems with limited force while at the same time winning the support of the population. This is a universally valid approach that can be utilized both in open war zones and in densely populated urban war zones.

Lessons Learned

During the United States’s involvement in Iraq, urban warfare turned out to be the main challenge. The battle for Fallujah demonstrated what could go wrong. Operation Vigilant Resolve was an unsuccessful attempt by the U.S. military to capture the city of Fallujah. Unable to control the situation, on the night of 4 April 2004, American forces launched a major attack to "re-establish security in Fallujah."27 In the opening days of the siege approximately a third of the population fled the city. Hospitals had to close and fighting broke out in large parts of central Iraq. On 9 April 2004, the U.S announced a ceasefire and called for negotiations between the Iraqi Governing Council, insurgents and city spokespersons. For the American troops the siege was a disaster because the use of “brute force” backfired politically. American forces only managed to gain a foothold in the industrial district to the south of the city, but on 1 May 2004, American troops withdrew.

Operation Al-Fajr was the second American attempt to take Fallujah. The battle involved the heaviest urban fight since the Battle of Huế City in Vietnam in 1968. Some 13,500 US, Iraqi and British troops were deployed outside the city. Some 3,000 – 4,000 insurgents who prepared spider holes, dug tunnels and trenches, built a large number of IED and booby-trapped buildings and vehicles, in defence of the city. By 13 November 2004, most of the fighting had ended, but sporadic fighting against pockets of resistance continued until 23 December. Operation Al-Fajr demonstrated that (short-term) military success in conquering a city is possible with brute force and search and destroy operations.

The second Lesson Learned was that after the overthrow of Saddam Hussein indigenous security forces and leaders could still play a crucial role. Prompted by Shiite and Kurdish leaders, the American president of the Coalition Provisional Authority, Paul Bremer, decided
to dissolve the official Iraqi armed forces and start a program of de-Ba’athification. As the entire Iraqi security apparatus and bureaucracy (mostly Sunnis) were dismantled, the responsibility for Iraq’s security was left entirely in the hands of the coalition forces. Sunni Arabs who are a demographic minority in Iraq believed that these measures were attempts to impose domination over them. This was a powerful incentive to start the insurgency.

The third Lesson Learned was that early planning for conflict termination by the stabilization and reconstruction forces of a country is a prerequisite for success. In Iraq the decision not to plan for a stabilization and reconstruction phase was based on the wrong idea that Iraq could pay for the reconstruction through its oil revenues. During the counter insurgency phase, stabilization and reconstruction measures were supposed to be used to win the support of the people. However, the American occupation force did not anticipate an insurgency when it invaded Iraq. Consequently, deployed forces were unprepared for the full-fledged insurgency that followed soon after the overthrow of the regime. The poor execution of operation Iraqi Freedom left the U.S. military with no other choice than to develop a new counter-insurgency doctrine. It became known as the “Petraeus Manual.”

A final Lesson Learned was that Western templates of state building did not take the dynamics of local conflicts into account. In Iraq, the Americans tried to create a stable, secure, democratic and functioning state. This attempt failed completely. As too few troops were initially deployed, the stabilization operations failed. Reconstruction was difficult if not impossible because of the dissolution of the old security forces and the old bureaucracy. Political power passed from Sunnis to Shiites and these, in turn, were looking to Iran for guidance and support.

**Field Manual 3–24**

These Lessons Learned provided a context for major doctrinal innovations. In conjunction with a U.S. Marine Corp team, General Petraeus and his staff produced Field Manual (FM) 3–24 on counterinsurgency operations. The new COIN manual drew heavily on the work of classical thinkers, including the experiences of Sir Robert Thomson in Malaysia and the French in Algeria in the 1905s. The French military theorist Galula had written *Counterinsurgency Warfare: Theory and Practice* in 1964. It built on Mao Zedong’s observation that “revolutionary war is 80 percent political action and only 20 percent military.” Contemporary Anglo-Saxon thinkers, such as John A. Nagl and David Kilcullen, were influential as well. Army Lieutenant Colonel Nagl co-authored the new counterinsurgency manual as part of a team overseen by General David Petraeus and led by his old West Point classmate Conrad Crane. Kilcullen was the Chief Strategist in the Office of the Coordinator for Counterterrorism at the U.S. State Department and later became a counter-insurgency advisor to General Petraeus.

The new Petraeus manual was built around two ideas, which were both drawn from doctrines of European colonial warfare. First of all, was the insight that protecting the population is key to success in any counterinsurgency campaign. At the same time, there is the recognition that insurgents will try to deprive the population of any sense of security. Second, was the insight that to succeed in counterinsurgency, armed forces have to learn and adapt more rapidly to changing circumstances than the enemy. America’s new counter-insurgency doctrine dramatically increased the performance of its troops in Iraq. A new clear, hold, and build approach was already showing some results before Petraeus arrived in Iraq, but as a new commander, Petraeus decided to apply it in all Sunni regions. Petraeus called this approach “the Sons of Iraq,” which consisted of recruiting, equipping and paying former militiamen for the fight against the local franchise of Al Qaeda. The Sons of Iraq approach spread the “Sunni Awakening” to other Sunni areas where the Americans and local leaders shared the same interests, i.e., the defeat of Al Qaeda.
The new Petraeus manual called for a different mindset and counter intuitive action. The manual observed that the admonition “Sometimes, the More Force Used, the Less Effective It Is” does not apply when the enemy is “coming over the barricades.” However, that thought is applicable when increased security is achieved in an area. In short, these paradoxes should not be reduced to a checklist; rather, they should be used with considerable thought. Other insights are “sometimes, the more you protect your force, the less secure you may be” and “the more successful the counterinsurgency is, the less force can be used and the more risk must be accepted.”

The original Petraeus manual from 2009 inspired subsequent publications like NATO’s *Allied Joint Doctrine for Counterinsurgency* of February 2011 and its update in 2016. The NATO publication introduced the new thinking on counterinsurgency to America’s allies. The doctrine emphasized the political nature of the counterinsurgency as well, by defining counterinsurgency as “the set of political, economic, social, military, law enforcement, civil and psychological activities with the aim to defeat insurgency and address any core grievances.” This aim can only be achieved by a comprehensive approach to crisis management. The Petraeus manual has been updated again in 2018. Other doctrinal innovations include the Comprehensive Approach and the “whole-of-government” approach. The latter integrates the collaborative efforts of US departments and agencies to achieve unity in effort towards a shared goal. The former integrates those efforts with partners, civil society (NGOs) and private sector activities. Both approaches are consistent with population centric operations, which require the harmonized use of economic, diplomatic, political and military instruments. Conceptually, this approach has some relevance for counterterrorism operations at home. As mentioned above, when fighting against individual terrorists or small cells in American or European cities, the use of excessive force might turn (parts of) the population against the authorities, whilst winning the “hearts and minds” requires a “whole of Government approach” for addressing justified grievances.

Unfortunately, doctrinal innovations are no guarantee for success. As the Afghan insurgency turned out to be more complex than the insurgency witnessed in Iraq, the American COIN doctrine developed for Iraq could not be easily transferred to the Afghan conflict theatre. A number of factors explain the failure of COIN in Afghanistan. First, Al Qaeda and the Taliban were intertwined and elusive adversaries. Second, compared to Afghanistan the sectarian and tribal divides were more complex. Because of this, local and allied leaders shared few common interests with the United States and its NATO allies. Consequently, as Fred Kaplan observed: “the problem (…) was that Afghanistan was not susceptible to COIN.”

**Prevention Through Deterrence**

The events that took place during the Battle for Mogadishu in 1993 demonstrated that terrorists and insurgents could deter an intervening force. When no vital interests are at stake, Western powers may choose to stay away from intervening in complex contingencies. Libya is a case in point. In 2011 NATO tried to achieve its objectives with airpower alone. After the fall of the Libyan leader Gaddafí, the country sunk into chaos, and there was no appetite to carry out an intervention with ground forces. France and the United States could have taken responsibility for the country after the regime change, but they did not do so because of the risks involved in fighting insurgents and terrorists.

The choice for air power and the use of proxies indicates that terrorists and insurgents can at times deter certain risky operations. However, there is no evidence that terrorists and insurgents can always deter an intervention. If vital interests are at stake for the intervenor, he is willing to take action and run considerable risks. This happened after the attacks of 9/11. President George W. Bush concluded that the Taliban provided Al Qaeda with a safe haven in
Afghanistan and that this constituted a security risk that could not be left unanswered. Consequently, he initiated *Operation Enduring Freedom*.

Deterrence can only be successful if the adversary believes that he has little or nothing to gain from aggression. If terrorists consider the prospect of fighting against an adversary using superior COIN and counterterrorism tactics so frightening that they refrain from using force at all, then the answer whether deterrence works is positive. However, few scholars and policymakers think that this is actually the case. Robert Trager and Dissislava Zagorcheva argue that the belief that terrorists cannot be deterred rests on the belief that terrorists are fanatics and irrational, are willing to die for what they consider a good cause, and lack instruments for creating counter deterrence. President George W. Bush reflected this view during his 2006 graduation speech at West Point: “Unlike the Soviet Union, the terrorist enemies we face today hide in caves and shadows (...) The terrorists have no borders to protect, or capital to defend. They cannot be deterred – but they will be defeated.”

However, Bush’s argument is seriously flawed and an underestimation of terrorist leaders. Terrorists are certainly fanatics, but terrorist leaders such as Al Qaeda’s Bin Laden and, after his death, Al-Zawahiri, and ISIS-leader al-Baghdadi are not irrational. They run complex international organizations, inspire their followers ideologically and religiously, develop new strategies in response to (partial) defeats, and manage to achieve at least some of their political objectives. As terrorist “Chief Executive Officers,” they exploit tribal, ethnic, and religious differences. They define goals, issue orders, and use modern management techniques. Whatever their objective, they motivate their followers to fight for their cause. In the eye of their followers and supporters, they are charismatic leaders fighting for a cause worth dying for. They have much in common with classical revolutionary leaders.

Trager and Zagorcheva argue that “even the most highly motivated terrorists … can be deterred from certain courses of action by holding at risk their political goals, rather than life of liberty.” They believe that this is possible for two reasons. Firstly, the relationship between states and non-state terrorists are often not zero-sum games. Secondly, states can influence their political aims. Trager and Zagorcheva believe that holding at risk political objectives is a crucial point. Robert Pape argued that even suicide terrorism can be deterred because they follow a strategic logic, i.e. “to inflict enough pain and threaten enough future pain to overwhelm the target country’s interest in resisting the terrorists’ demands.” This requires classical counter measures such as limiting access to the target area, taking into account resentment with regard to foreign occupation of the terrorist’s national homeland, and preventing polarization in the West.

Ron Radlauer argued that punishing the innocent could, in theory, deter suicide bombers. In Israel, destroying the homes of the suicide bombers' family is meant to do this. At the same time, Radlauer concludes that this has in practice little effect. As it is unlikely that destroying homes will win the “hearts and minds” of the populace, this comes as no surprise. Gaining physical access to the general target area is the only genuinely demanding part of an operation, and a key part of the motive for suicide terrorism.

Israel is arguably most advanced in its thinking on deterring violent extremist groups. Shumuel Bar considers “intelligence dominance” an important deterrent. This concept refers to the perception of terrorists that the opposing state has superior intelligence capabilities and consequently the ability to attack them at will. Bar argues that the Israeli authorities have deliberately created the image of an “intelligence superpower.”

Mark Vinson argued that “ever since achieving statehood in 1948, deterrence has stood as a pillar of Israel’s national defense strategy.” Deterrence operations, aimed at keeping political violence on an acceptable level, now form an integral part of Israel’s defense planning. Deterrence operations can take the form of “measured retaliation” or “massive retaliation.” Both aim to restore deterrence or dissuade further escalation. Conceptually, these concepts are similar to the COIN concept of maneuver warfare and attrition or brute force. The main
difference is that the COIN concept is translated into deterrence theory. The distinction between deterring attacks and inter war deterrence is important as well. Intra war deterrence has, in the Israeli context, been defined as the ability to prevent further escalation or de-escalate the conflict and is based on the Israeli experience of periodic wars with its adversaries and the desire to prolong the interwar period as much as possible.

Measured or flexible retaliation seeks to maintain deterrence at the current level and prevent further escalation of the conflict. Massive retaliation seeks to reset deterrence through massive and overwhelming force. Targets are the violent extremist organizations or their proxies. The last massive Israeli response operation was Operation Protective Edge (2014) targeting Hamas in Gaza – an operation which saw more than 2,000 Palestinian deaths and more than 10,000 injured. This has led to accusations that Israel had violated international humanitarian law and international human rights law.

Deterrence theory makes a distinction between two forms of deterrence. Deterrence by denial involves denying a group from achieving its political objectives, whilst deterrence by punishment involves the (partial) destruction thereof.

Deterrence by denial can take different forms. Some examples are:

- The hardening of potential targets, upgrading of border controls, the reinforcement of cockpit doors in passenger aircrafts and tighter border controls are relatively simple and effective means to deter terrorists from attacking objects. Due to excessive safety measures, American embassies are no longer rewarding targets. The same holds true for most US military facilities abroad.
- Following attacks on Christmas markets and other public events in Europe, bolders, roadblocks or even walls have been introduced to deter attacks with trucks. However, some people consider roadblocks as a form of collective punishment, thus weakening its deterrent effect. This happened in Israel where Palestinians see roadblocks and walls as injustice.
- Restricting access to the commodities needed for the manufacturing of biological, chemical and radiological weapons explains the limited number of attempts to carry out attacks with CBRN-weapons. Potential perpetrators find it increasingly difficult to buy sufficient quantities of the required ingredients for bomb-making in shops and from wholesalers.
- Active counter measures, such as Israel’s Iron Dome missile-defense system, are designed to counter missile attacks. During the massive attacks by Hamas in early May 2019, the Israel Defense Forces claimed that its antimissile system was 86% effective during a Hamas bombardment of 690 rockets, suggesting that Hamas’ tactics had a relatively minor effect.

Statistical data show that deterrence by denial is often effective. Before carrying out an attack, terrorists will make an assessment of the likelihood of success. They will attack soft targets when hard targets cannot be hit. According to the Dutch Intelligence Service (AIVD), this explains why 85 percent of 112 failed and successful attacks in Western countries were aimed at soft targets. Only 8 percent of the attacks were aimed at targets which were to some degree protected, whilst 5 percent of the attacks were aimed at highly protected or hard targets.

Deterrence by punishment is more difficult and will usually involve direct attacks against targets that are of great value for terrorists:

- Attacks on the adversary’s bases, command, control, communications (C3) and intelligence systems could affect a group or individual’s motivation. Attacking C3 systems could introduce uncertainty.
- C3-attacks and eavesdropping could deter terrorist leaders from using cell phones, satellite communication and computers.
Pressuring the host population is one form of indirect coercion. But this tactic is at odds with winning the “hearts and minds” of the populace. This tactic was unsuccessful during Israel’s confrontations with Hamas and Hezbollah where Israel was seen as an occupying force that violated human rights. In general, disproportional counterterrorism operations can increase the support of the population for a terrorist organization.

More difficult is targeting patron support. Targeting the sponsoring patron could compel him to refrain from offering assistance to terrorists. This worked for a time well with Hezbollah and Fatah which were dependent on Iran, Lebanon, the Palestinian Authority and Syria. It did not affect Hamas which was relatively independent. For national counterterrorism operations this means cutting off extremists from their base by targeting their sponsors – something that can be effective.

Targeted killing is an extreme form of deterrence by punishment. The same holds true for the destruction of terrorist’s facilities as it can diminish individual motivation and influence group behavior. The American drone-attacks on Al Qaeda and Taliban facilities in the border region of Afghanistan and Pakistan are examples of this tactic. Since deterrence by punishment is likely to have a detrimental effect on the population, it carries with it the same kind of disadvantage as the COIN concept of attrition or the use of brute force. For that reason, an interesting new form is deterrence by de-legitimation. This form of deterrence seeks to raise “the costs of participating in terrorism by challenging the normative, religious, and socio-political rationales individuals rely upon when participating in violence.” It is aimed at the political, ideological and religious rationale of terrorist behavior.

This involves the creation of a credible counter narrative that questions the beliefs and guiding principles of terrorists. As most terrorists do not have deep knowledge of religious and ideological issues, one might expect that some of them are receptive to alternative visions, especially if those visions come from trusted experts. Some jihadi scholars and former practitioners of terrorism have questioned terrorism. For example, the early Al-Qaeda ideologue Sayyid Imam Sharif (better known as Dr Fadl) backtracked in 2007.

Since terrorists will try to innovate their responses, complete deterrence is impossible. Moreover, in contrast to democratic governments, terrorists do not have to play according to the rules. On the contrary, they will make use of the fact that authorities in democracies will have to fight, as it were, with one hand tight on their back, following the rule of law and observing human rights. Bruno S. Frey has argued that deterrence is based on a negative approach: “terrorists are threatened with punishment if they continue their activities. Coercive action is answered by coercive action.” This can result in a negative sum game between the parties involved. In contrast to deterrence by denial, escalation is certainly a risk that should be taken into account when considering deterrence by punishment strategies.

**COIN Tactics and Parallel Societies**

As has been mentioned before, COIN is population-centric, whilst counterterrorism focuses on targeting violent extremists and terrorists. In Europe, few extremists are lone wolves. Most extremists live and radicalize in extremist milieus or hubs.

Can extremists hide in neighborhoods? In major European cities a high degree of segregation of different population groups has been observed. Contact with the indigenous population is least in neighborhoods with large numbers of immigrants and ethnic minorities. Those neighborhoods can become safe havens for jihadists. In those places, jihadist hubs can be established. One report concluded that in Europe, “the formation of hubs often happens around organized structures (militant Salafist groups, radical mosques), charismatic
personalities or, in some cases, tight-knit groups of friends." The report mentions a case of radicalization in the town of Hildesheim, in the German state of Niedersachsen. Seventeen individuals from Hildesheim travelled to the Caliphate of ISIS while others were engaged in militant activities in Germany. Extremists were mobilized by a small group of Salafists organized in the Deutsch-Islamischer Kulturverein (DIK – German Islamic Cultural Association). Gradually, the DIK became a well-known center for like-minded Muslims in Germany. A similar breeding ground could be found in Molenbeek, a suburb of Brussels, Belgium. A police report showed that in this suburb a number of organizations had links with terrorists. Sevran, a Parisian suburb that is home to more than 70 nationalities, is another example. The French Cities Minister, Patrick Kanner, stated that there are “a hundred” French neighborhoods like Molenbeek. In the Netherlands problems concentrate on a limited number of districts in the four biggest cities, Amsterdam, Rotterdam, Utrecht and The Hague. Across Europe, a number of neighborhoods have developed into parallel societies with de facto “no go” areas for the police. The fact that these quarters (partly) elude government control allows the strengthening of such parallel societies where terrorists can hide.

Conceptually, COIN tactics can be applied when fighting extremists in parallel societies and no-go areas. To do so, an excellent information position is paramount. Intelligence should enable the authorities to identify cells and individuals. Those individuals should be isolated from their support base. At the same time, the “hearts and minds” of the local populace should be won and counterterrorism operations should refrain from the use of excessive violence as this might only facilitate further radicalization.

Conclusions: Counterinsurgency and Counterterrorism in Western Democracies

As mentioned before, sound doctrines and correct strategies are prerequisites for success. The strategy should set the political objectives; the doctrine helps translating those objectives into military action. The same holds true for domestic counterterrorism operations by police forces. Without a clear strategy and clear doctrinal principles, counterterrorism is doomed to fail. The same holds true if counterterrorism lacks superior intelligence capabilities or when a “whole of government” approach is absent.

Military establishments have learned that insurgency and terrorism are part of a broader political struggle with the populace as center of gravity. Consequently, both COIN and counterterrorism doctrine should be population centric. Protecting the population is the key to success in any counterinsurgency campaign. A “hearts and minds” campaign is a prerequisite for gaining the support of the population. This should not be confused with softness. It is an essential activity to prevail in a political struggle. It requires responsible leaders to abstain from harsh rhetoric stigmatization of sectors of society vulnerable to terrorist appeals and refraining to contribute to polarization between majority and minority groups in society. Political leaders ought to respect groups identities and grievances, and should take socio-economic measures to take away (some of) the grievances. At the same, they should be aware that jihadists and other militants will try to deprive the population from a sense of security.

The US military makes a clear doctrinal distinction between COIN and counterterrorism operations. A key difference between these is that insurgents rely on support of the populations whilst terrorists are individuals or isolated groups or cells without broad public support. The difference is that COIN requires a “hearts and minds” campaign, whilst counterterrorism requires search and arrest or destroy tactics without causing too much trouble for the population. In sum, the nature of the threat will define whether COIN or counterterrorism tactics should be applied.

Another lesson learned is that deterrence can be effective. Most terrorists are rational actors who make cost-benefit calculations. Thus, increasing the costs of action by the deterring side is important. The party which deters should hold something at risk that the adversary values.
Deterrence by denial is relatively simple; deterrence by punishment is more difficult; here the analytical literature can cite only few successes. The only achievement might be Israeli-style “intra war deterrence” or the ability to control escalation or deter excessive violence. Deterrence by punishment will probably have detrimental effects during domestic counterterrorism operations.

In sum, national authorities can draw important lessons from the vast experience of the military with COIN and counterterrorism operations. Unfortunately, due to cultural differences between the military and civilian national security establishments, there is a natural tendency to ignore those Lessons Learned. An important obstacle is the perception that the military rely too much on the use of force. However, the experience with military COIN and counterterrorism operations reveals that this perception is wrong. This contribution argued that the military are very well aware of the political environment in which COIN and counterterrorism operations take place. They understand that this environment requires a completely different attitude in which the use of force plays a subordinated role. Finally, national counterterrorism efforts will greatly benefit from doctrine development. Like the military, Lessons Learned and conceptual approaches should be captured for improving future counterterrorism operations. If not, valuable knowledge might be lost.

Prof. Rob de Wijk is founder of The Hague Centre for Strategic Studies (HCSS) and Professor of International Relations and Security at the Faculty Governance and Global Affairs (ISGA), Leiden University. He studied Contemporary History and International Relations at Groningen University, and wrote his Ph.D. dissertation on NATO’s “Flexibility in Response” strategy at the Political Science Department of Leiden University. Rob de Wijk started his career in 1977 as a freelance journalist and later became head of the Defense Concepts Department of the Dutch Ministry of Defense, head of the Security Studies at the Clingendael Institute, and Professor of International Relations at the Royal Netherlands Military Academy. He wrote extensively on security affairs, including The Art of Military Coercion (Amsterdam: AUP, 2004) and Power Politics (Amsterdam: AUP, 2015).
Appendix: A Checklist of Lessons Learned from Counterinsurgency and Counterterrorism Experiences

Military COIN and counterterrorism doctrines gained from operations by major Western powers contain some Lessons Learned which should be taken into consideration for domestic counterterrorism operations as well. Some of these are:

- Major terrorist groups use constructive activities to gain the support of (parts of) the population and engaging in destructive activities to deter and fight the adversary. They tend to use asymmetry tactics to confront the adversary not on his own terms. It is a tactic of the weak that can be very effective. Underestimating insurgents and terrorists because friendly troops possess superior firepower and technology is extremely dangerous. Technology plays a supporting role at best.
- Military victories will therefore never be spectacular. Rather, victory will be achieved by a sequence of small successes.
- The planning of any COIN operation requires strategy, based on an analysis of the type of conflict, its implications, and the method to stop, neutralize or reverse actions of the opponent. To achieve the desired end state, clear political objectives must be defined.
- Attrition and deterrence by punishment is based on repression and destruction of the adversary. But in most cases, this will lead to accusations of barbarism and war crimes and abhorrence among the populace.
- Urban warfare can be extraordinarily destructive, especially if a strategy of attrition is applied. Therefore, small-scale urban operations should be given preference, actions involving traditional policing operations to prevent and contain the outbreak of violence alongside small scale (covert) counterterrorism operations.
- In unconventional warfare it is only through the physical control of an area or the isolation of the opponent that military objectives can be met. This requires the use of small units, which ultimately need to occupy terrain on the ground.
- Direct action to gain control over an area involves cutting off logistics (isolation), cordon operations, and search-and-destroy operations. In those cases, minimal use of force works best, because the insurgents seek to demonize intervening force or local authorities’ use of excessive force.
- In unconventional warfare two levels are most important: the strategic level for overall direction and the technical level for the actual war fighting. The strategic level should also involve political and diplomatic actions.
- Intelligence and skills are important factors for success.

American, British and NATO manuals broadly agree on a number of principles that should be taken into account when executing COIN operations that could also improve domestic counterterrorism operations:

1. The people:
   - Carry out “hearts and minds” activities.
   - Provide the conditions for economic, political and social reforms.
   - Provide essential services and address the core grievances of the insurgency.
   - Protect the local, neutral, and sympathetic parts of the population against insurgents.
   - Safeguard key infrastructure.

2. Isolate the insurgents:
   - Gain the support of the populace.
• Physically and psychologically separate insurgents from the population.
• Deny the adversary active and passive support.
• Use and train local workers and materials to rebuild and provide a sustainable economic and social system.

3. Neutralize the insurgents:
• Eliminate the ideological, religious and logistical support system of the insurgents, including the prevention of external support from other organizations and countries.
• Cut off the insurgents from (food) supplies and recruits to separate them from the population.
• Eliminate the adversary’s intelligence and communication network.
• Carry out direct action against terrorist cells and individuals, their ideological, religious and logistical support with small scale, covert operations and minimum use of force.
• The use of force should be selective and proportionate and should not upset larger parts of the local population.
• Restraint is key. Too much force will only increase the support for terrorists and will make it more difficult to win the “hearts and minds” of the population.
• Deterrence by denial, i.e. influencing the cost – benefit calculus of extremists should play an important role in the overall strategy. Terrorists might dream of catastrophic attacks, but can be deterred from doing so.
• Excessive force might be needed to reset deterrence, but this can only be effective if the terrorist targets experience large-scale violence by violent extremist organizations. In all other cases a flexible, measured response is needed. In case of small cells and individuals the best method is small scale, preferably covert operations.
Endnotes

4 US Joint Chiefs of Staff, Joint Publication 3-26 Counterterrorism, 24 October 2014, p. vii.
5 Joint Publication 3-26 Counterterrorism, V-3 – V-5.
8 Colombo, Roberto, ‘Choosing the Right Strategy: (Counter) Insurgency and (Counter) Terrorism as Competing Paradigms,’ Security Distillery, 15 February 2019. Available at: https://thesecuritydistillery.org/.
10 Pew Research Centre, Muslim Publics Share Concerns about Extremist Groups, 10 September 2013; Available at: https://www.pewglobal.org/2013/09/10/muslim-publics-share-concerns-about-extremist-groups/
15 The Interdisciplinary Research Program on Root Causes of Human Rights Violations (PLOOM) of Leiden University, the Netherlands, produced an annual World Conflict and Human Rights Map; Oxford University Press publishes the SIPRI Yearbooks.
18 See, for example, the British Army Field Manual Countering Insurgency; Vol. 1, Part 10, Army Code 71876, October 2009.
23 Hénin, Nicolas, ‘The Caliphate is Gone, but Islamic State has a New Plan,’ The Guardian, 7 May 2019.


AJP-3.4.4., pp. 1-4

AJP 3-07, pp. 3 - 4.


Don Radlauer, ‘Rational Choice Deterrence and Israeli Counter-Terrorism’, Intelligence and Security Informatics, 2006, pp. 609-614. Available at: https://link.springer.com/chapter/10.1007/11760146_65


46 Bill Bostock, ‘Israel’s Iron Dome missile-interception system stopped 86% of an enormous rocket barrage despite Hamas claims to have overwhelmed it’, Business Insider, 7 May 2019; Available at: https://www.businessinsider.nl/hamas-claim-beat-iron-dome-missile-interceptor-israel-disagree-2019-5/?international=true&r=US

47 Algemene Inlichtingen en Veiligheidsdienst (General Intelligence and Security Service of the Netherlands) Doelwitten in beeld, Zoetermeer: AIVD, 2019, p. 22.


Bibliography


*Allied Joint Doctrine for Counterinsurgency* (AJP-3.4.4.), February 2011.


Colombo, Roberto, ‘Choosing the Right Strategy: (Counter) Insurgency and (Counter)Terrorism as Competing Paradigms,’ *Security Distillery*, 15 February 2019. Available at: https://thesecuritydistillery.org/.


Department of the Army, FMI 3-07-22 *Counterinsurgency Operations*. Department of the Army, October 2004. Available at: https://www.hsdl.org/?view&did=468442


Metz, S., *Learning from Iraq: Counterinsurgency in American Strategy*. Carlisle, PA:
US Joint Chiefs of Staff, Joint Publication 3-26 Counterterrorism, 24 October 2014.
Web-based Resources


Pratt, Simon. What is the difference between counterinsurgency and counterterrorism? (December 2010,). E-International Relations Students. https://www.e-ir.info/2010/12/21/what-is-the-difference-between-counter-insurgency-and-counter-terrorism/

Chapter 6

“Killing Them to Save Us”: Lessons from Politicide for Preventing and Countering Terrorism

Clark McCauley

This chapter reviews and extends the analysis of mass political murder advanced by Chirot and McCauley, then applies this analysis to understanding and countering terrorism. The justification for this application is that both politicide and terrorism target civilians in the context of asymmetric conflict. Three generalizations emerge. Politicide and terrorism cannot be understood or countered without (i) studying both sides in the conflict, (ii) separate studies of leaders, perpetrators, and mass sympathizers, and (iii) acknowledgment of the threats and grievances perceived by both sides. The chapter concludes with implications for fighting the war of ideas against jihadist and right-wing terrorists.

Keywords: genocide, mass murder, politicide, democide, terrorism, radicalization, asymmetric conflict, political extremism, right wing extremism, prevention, Islamist extremism, countering violent extremism (CVE)
In this chapter, I follow Chirot and McCauley\(^1\) in focusing on the mass killing of civilians - political murder - as practiced both by stronger groups attacking weaker groups (genocide, democide, politicide) and weaker groups attacking stronger groups (terrorism). As explained in the first section of the chapter, I will refer to politicide when referring to the former. The premise of this chapter is that both politicide and terrorism aim to kill civilians. It is possible therefore to find parallels between the psychology of politicide and the psychology of terrorism. These parallels can offer us further suggestions about how to prevent and counter terrorism.

The chapter begins by expanding the United Nations (UN) definition of genocide to include attention to mass murder conducted against political enemies (democide, politicide). Special attention is given to mass murder in aerial bombings and mass murder in ungoverned spaces. A threat-based model of motivation for politicide is then introduced and applied to different actors involved in politicide: leaders, perpetrators, and the masses (general public). The second section examines possible predictors of politicide, followed by a third section that considers possible interventions against politicide, then a fourth section summarizing what we know about politicide. The sections five and six apply a novel understanding of politicide to better understanding and countering terrorism. The concluding section offers three generalizations about how to counter terrorism more effectively.

Mass Political Murder: Genocide, Democide, and Politicide

The UN definition of genocide is “acts committed with the intent to destroy, in whole or in part, a national, ethnic, racial or religious group.” This definition emerged from negotiations and compromises among UN member states in ratifying the 1948 Convention on the Prevention and Punishment of the Crime of Genocide.\(^2\)

The UN definition applies to the Armenian genocide of 1915 and the Nazi genocide of the Jews during WWII. It applies also to Hutu killing Tutsi in Rwanda in 1994, but misses the many Hutu moderates killed by Hutu militants. It does not comprehend Stalin’s targeting of the kulaks, a prosperous peasant class. And it misses entirely the millions of “Cambodians with Vietnamese minds” killed by the Khmer Rouge between 1975 and 1979. In general, the UN definition excludes political groups killed in programs of political suppression.

Recognizing the limitations of the UN definition of genocide, Chirot and McCauley argue that the phenomenon of interest should be referred to as “mass political murder.”\(^3\) They assume that the psychologies involved in killing everyone in a village of a hundred are basically the same as killing millions of Armenians or Jews. The logic of this assumption is that millions are not killed in one day or in one episode of killing. Millions are killed in the summation of many episodes of killing hundreds or thousands, episodes that are spread geographically as well as in terms of duration.

Rummel has advanced the term democide to refer to mass political murder. “Democide’s necessary and sufficient meaning is that of the intentional government killing of an unarmed person or people.”\(^4\) Rummel explicitly excludes from this definition government execution of individuals for internationally recognized very serious crimes such as murder, rape, and treason. Unfortunately, Rummel’s definition of democide excludes mass killing in ungoverned spaces such as the Democratic Republic of the Congo, as described below. Relatedly, Harff and Gurr have advanced the term politicide to refer to mass political murder:

“The essential quality of all these episodes is that the state or dominant social groups make a concerted, persistent attempt to destroy a communal or political group, in whole or in part. …In genocides the victimized groups are defined primarily in terms of their communal characteristics. In
politicides, by contrast, groups are defined primarily in terms of their hierarchical position or political opposition to the regime and dominant groups.”

Politicide, like democide, goes beyond the UN definition of genocide to include mass killing of political enemies who are not defined by ethnicity or religion. Politicide, like democide, can include the Hutu’s killing of moderate Hutu, Stalin’s targeting of kulaks as an economic class, and Khmer Rouge’s killing of “Cambodians with Vietnamese minds.”

Unlike democide, however, politicide does not require, by definition, that a government is behind the killing. “In politicides, by contrast, groups are defined primarily in terms of their hierarchical position or political opposition to the regime and dominant groups.” In politicide, the targets are groups defined in terms of their political status, that is, usually their opposition to a ruling group.

This is a definition that can be applied to mass killings in ungoverned spaces. In this chapter, therefore, I aim to understand the psychology of politicide, as Harff and Gurr have defined it, and to apply this psychology to the context of terrorism, to better understand and prevent terrorism.

Here it is useful to emphasize an aspect of politicide that is key to psychological analysis: politicide is killing by category. The targets of politicide are not determined by any individual characteristics or individual behaviors but by their link or membership to a social group. The group is targeted as a category, making equally of old and young, male and female, politically active and politically inert targets. The psychology of politicide must make sense of killing by category.

**Mass Killing in Aerial Bombings**

A salient but controversial example of killing by category is the aerial bombing of enemy population centers (for citations supporting the figures in this section, see McCauley; for the history of the controversy over city bombing see Maier). In WWII, Germans bombed English cities and the air forces of the UK while the US bombed German cities. English deaths from German bombs were about 40,000; German deaths from British and American bombs were about 400,000. In the war against Japan, the US firebombed 58 cities, killing about 900,000 Japanese civilians. The atomic bombs against Hiroshima and Nagasaki, dropped in August 1945, killed an additional 105,000 persons.

City bombing, especially in times of war, kills mostly civilians: women, children, and the elderly as military-age men are mostly on the front lines. City bombing thus fits the definition of politicide: mass killing of civilians targeted for their political status and opposition to the power that targets them. In World War II, city bombing was often referred to as “terror bombing” because many believed that the civilian suffering under aerial bombing (“terror”) would lead citizens to demand that their leaders surrender.

It appears to have been easy to order young men to engage in city bombing. I could find no record of American British or German aircrews refusing orders to bomb cities, or even protesting against this kind of mission. No doubt it helped that city bombing was conducted from high altitudes, to avoid flak and enemy fighters. Flying miles above a city, the suffering brought by incendiaries and high explosives are lost from view.

The logic of killing enemy civilians is the logic of the modern nation state. Beginning with the French *levée en masse* in 1793, wars are fought by industrial states that conscript soldiers and organize every kind of production and technology for the war effort. The distinction between soldier and civilian has been eroding since 1793 and an end to this trend is not in sight. Erosion of this distinction has not been lost on those who challenge the state as terrorists.
Mass Killing in Ungoverned Spaces

In much of the traditional literature, politicide has been seen as government work. A group in possession of the instruments of the state attempts to eliminate a weaker group, either by pushing its members out of the country or by killing them directly. It is usually government power, government planning, and government organization that make mass executions, ethnic cleansing and mass deportations possible. One is tempted to say that the difference between a deadly ethnic riot and a politicide is the steady application of government power.

In the 21st century, however, it has become clear that mass political murder can also occur in the absence of government power. Between 1997 and 2008, more than five million people died in the Democratic Republic of the Congo (DRC) and millions more were displaced as internal or external refugees. Like most reports from the DRC, the death toll is disputed - it may amount to “only” three million people. Many deaths in the DRC have been the result of malnutrition and disease among those displaced, especially children.

Violence in the DRC occurs at the intersection of civil war, tribal conflicts, conflicts over mineral resources, and interventions by armed actors from neighboring countries. Armed militants from one faction attack villagers of another faction - pillaging, raping, burning, and killing. In the welter of these complex conflicts, it is difficult to determine the motives, but there were signs at least of material gain, status, and security threats represented in reports of pillaging and rape, anger and revenge, as well as killings aimed at outright extermination. Notably the violence included a genocidal campaign by Bantu tribes against pygmy peoples in eastern DRC provinces. This particular campaign appeared to include elements of perceived ‘pollution threat’ insofar as the Bantu are said to see pygmies as not quite human.

After years of violence in the DRC, the predominant motive for killing for some may simply be revenge. It appears that, in the absence of government authority, DRC suffers multi-sided politicides in which bands of armed men destroy the shelter and sustenance of those not killed outright. In 2019, mass killing in the DRC continued, both by government security forces and militias, and by many of the more than 140 armed groups operating in the eastern provinces of the DRC.

Four Kinds of Perceived Threat that can Lead to Politicide

Many observers have pointed to perceived threat as a motive or justification for ethnic cleansing, genocide, and mass political murder. Drawing from this literature, Chirot and McCauley identified four types of threat associated with killing people by category.

- **Material threat** is the perception that another group blocks “our” economic progress; the convenient response is to eliminate the source of frustration. The US’ removal of the Cherokee from Georgia in 1838, for instance, occurred after gold was discovered on the tribe’s ancestral lands. Evicting the Cherokee from their homes and submitting them to a forced march through unfamiliar territory resulted in many deaths. In this and other cases, removal has been a powerful means of mass political murder.

- **Status threat** is the perception that another group has challenged “our” superior status; anger and revenge are the likely response, as in the years 1904 to 1908, when German colonial military forces killed most of the Herero - about 60,000 people - after members of this tribe had overwhelmed a small German garrison in Southwest Africa.

- **Security threat** is the perception that it is “them or us” Fear drives the violence, as was seen in the mutual massacres and expulsions of Serbs and Croats in the 1990s dissolution of Yugoslavia. Another example is Stalin’s extermination of the kulaks, who owned enough land to hire laborers and buy machinery. Stalin saw these small-scale capitalists as a mortal threat to his Communist Revolution. Soon, the operational definition of kulaks came to include anyone opposing development of state-controlled collective farms. In the 1930s, perhaps a
million kulaks died in direct executions or in gulags or during and after deportations to Siberia.  

Fourth and finally, pollution threat is the perception that another group is contaminating “our” ethnic, religious, or ideological purity. A well-known example is Hitler’s fear of Jewish pollution of the Aryan race. The distinctive emotion associated with pollution threat is disgust, which was represented in the Nazi’s descriptions of Jews as virus, lice, cockroaches, and rats. These epithets convey not just inferior animal essence, but disgusting animal essence associated with filth and garbage. The action tendencies associated with disgust are distancing and elimination; humans try to avoid viruses, lice, cockroaches, and rats, and to exterminate them if contact cannot be avoided.

Perception of a bad essence is a deep form of dehumanization. A bad essence cannot be reformed or re-educated; it can only be eliminated. All those who share the bad essence become legitimate targets, as all cockroaches are a target - large and small, old and young, whether they have raided our pantry or not. Pollution threat rationalizes killing by category.

The four types of perceived threat often overlap. Whites in the state of Georgia wanted Cherokee lands but were also disturbed by rising Cherokee education and prosperity and by beginnings of intermarriage between Cherokee and white settlers. That is, white Georgians felt not only under a material threat, but also a status-inversion threat, and a racial pollution threat. Similarly, the German Nazis felt material threat in the commercial success of Jews in business and banking, and felt a status threat from Jewish success in universities and the arts. Once mass killing of Jews had begun, Nazis also felt a security threat: Jews and their sympathizers would surely seek revenge if the Final Solution faltered.

For Stalin, the kulaks represented a material threat (they resisted grain requisitions), a status threat (they competed with Communist Party officials for influence in rural areas), and a pollution threat (they spread capitalist ideas; some even tried to join the Communist Party). Thus, although the four motives for politicide can be distinguished, and any given episode of mass killing may emphasize one motive more than another, it appears unlikely that any politicide can be explained in terms of response to only a single motive, a single form of threat. The four kinds of threat are usually mutually reinforcing; pollution threat in particular eases the way to killing by category. Finally, it is important to recognize that the four kinds of threat are associated with strong emotions, notably including fear, anger, and disgust.

Perpetrators, Leaders, and Masses

It is easy to talk about the motives of those who perpetrate mass killing, but who specifically are the perpetrators? Studies of politicide have found that many of the perpetrators of violence have joined in the killing for personal reasons that had nothing to do with intergroup threat. Some join out of habitual obedience to authority and fear of punishment if they did not join. Some join for the status and power that came from having a gun in their hands. Some join for salary or loot, for access to alcohol and rape, for comradeship, or to escape problems at home or with the law. The killers may indeed perceive a threat toward their own people. Presumably many of their people feel the same threat - but only few are taking part in the killing.

The Khmer Rouge forces that took Phnom Penh in 1975 numbered about 75,000 - about four percent of the 1.8 million Khmer Cambodian males between the ages of 15 and 64 in 1975. Although relatively few, the Khmer Rouge in 1975 controlled a nation of 7.5 million and in three years killed at least 1.6 million people.

Rwandan genocidaires numbered about 200,000, about 17 percent of Hutu males between the ages of 18 and 54 in 1994. In 100 days, the genocidaires killed at least 500,000 Tutsi and moderate Hutu.

For the deaths of about six million Jews, Roma, Slavs, and Nazi opponents during WWII, it is not easy to define perpetrators or estimate their numbers. The following quotation offers
the only numerical estimate I could find. “Dieter Pohl of the German Institute for Contemporary History estimates that more than 200,000 non-Germans - about as many as Germans and Austrians - ‘prepared, carried out and assisted in acts of murder.’”25 If German and Austrian perpetrators were 400,000, they would amount to two percent of 24 million German/Austrian men between the ages of 15 and 65 in 1939.26

The numbers for perpetrators - Khmer Rouge, Hutu, German/Austrian - are at best approximations that can be contested, but their general magnitude in relation to population numbers is revealing. In each case, the perpetrators represent only a small percentage of male adults who might have been perpetrators: two percent of Germans/Austrians, four percent of Cambodians, 17 percent of Rwandan Hutu. Similarly, the 600,000 men who served in US Army Air Force bombers in WWII, a maximum estimate of those who joined in city bombing, totaled only about two percent of US male adults.27

These small percentages indicate that perceived threat may be necessary for joining in mass killing, but it cannot be sufficient. The great majority of adult males who perceive an enemy threat never join in mass killing of the enemy. Perpetrators of politicide are a small minority of the people they claim to be defending.

If threat is not a sufficient explanation for the perpetrators, whose contribution to politicide is explained by perceptions of the four kinds of threat? The obvious answer is that the elites and leaders behind the perpetrators believe that they and their people are threatened with material loss, status loss, security loss, and “pollution.” The pronouncements of Turkish leaders, Hitler, Pol Pot, and the Hutu Radio Milles Collines make clear that those directing the Armenian, Jewish, Cambodian, and Rwandan politicides saw their victims as mortal threats to their own power and to the survival of their people. With regard to the perceptions of these leaders, only the Turkish case remains controversial (but see Akcem).28

What about those who are neither perpetrators nor leaders? Do they perceive the same threats as their leaders do? Do they support the violence that their leaders organize in the name of group survival? Polling data from before and during a politicide are difficult to come by. This is a research issue for the future. If politicide is perceived as likely, or even just begun, it may be possible to complete at least an internet poll to take the temperature of the general population of the stronger side, to determine the attitudes of the stronger toward the weaker and perhaps even the extent of support for cleansing or killing the weaker.

So how does a perceived threat make politicide possible? Threats perceived by leaders, not only to the welfare of their people but to their own power and status must surely count, or government power could not be organized for mass murder. Threats perceived by the actual killers is likely - not least as justification for their killing, but more personal motives are required to mobilize the few killers from among the many who feel the threat posed by a minority group. For the great majority of the stronger side who are neither leaders nor killers, we simply do not know the extent to which they supported the killing. There are always a few righteous men and women - true heroes - on the stronger side who risk their lives to save some of the weaker. How many disapprove of politicide but are not ready to risk their lives as rescuers, we do not know.

An important implication here is the realization that “they” are not all killers, they are not all alike. It is misleading to say that the Turks committed genocide against the Armenians, that the Germans committed genocide against the Jews, that the Hutu committed genocide against the Tutsi - accuracy requires less generalization and more specificity.

More specifically, the Young Turks political party committed politicide against the Armenians, including encouraging Kurds to attack Armenians. Hitler and the Nazi party committed politicide against Jews, Roma, Slavs, political opponents, and the disabled. A party of Hutu extremists committed politicide against Tutsi and moderate Hutu. The Khmer Rouge, a political party and its army, committed politicide against minority ethnicities (Chinese, Cham, Vietnamese) and against “Cambodians with Vietnamese minds.”
The important point here is that whole-group generalizations cannot be correct, there is always variation with a population as large as an ethnic or a national group, or even within a political party as large as the Nazis or the Khmer Rouge. To indulge in whole-group attributions is to misunderstand the problem of politicide and to throw away the possibilities for preventing politicide that come with recognition of divisions within the group in whose name mass murder is accomplished.

**Forecasting Politicide**

It is easy to notice two factors in common among the greatest politicides of the 20th century. These cases include Turks killing Armenians; Nazis killing Jews, Roma, Slavs, and political opponents; Khmer Rouge killing “Cambodians with Vietnamese minds” and ethnic minorities; Hutu killing Tutsi and moderate Hutu; and the back-and-forth killing in the DRC.

In each of these cases there was war, interstate war, or civil war, when mass killing occurred. War strengthens popular support for government, strengthens government control of news and information of every kind, raises the specter of “the enemy within,” and desensitizes citizens to death. If our own people are dying, how much can we care about the deaths of those who threaten our people?

In each of these cases, there had been earlier examples of killing by category on a smaller scale, that is, targeting people on the basis of who they were rather than because of anything they had done. Turks, Germans, and Hutu had killed Armenians, Jews, and Tutsi in various episodes years before large-scale mass killing began. In Cambodia, the Khmer Rouge began forcible removal of town and city populations to rural labor camps in 1973-74, months before winning and emptying the capital Phnom Penh in 1975. As already noted, mass killing in the DRC followed years of back-and-forth attacks on villagers. Past and recent killing by category is a warning of more to come, consistent with the well-worn psychology that “the best predictor of future behavior is previous behavior of the same kind.”

A third factor next to war and historical antecedents contributing to politicide is political and material support from another country. Germany supported the Young Turks; China supported the Khmer Rouge; France supported Habaryirama’s Rwandan Hutu government, even sending French troops to help fight the invading Rwandan Patriotic Front (RPF). Rwanda and Uganda have supported militant factions in the DRC. Only the Nazi politicide did not need outside support.

War, previous politicide, and foreign support are relatively nonspecific warning signs for politicide. Verdeja reviewed efforts to predict genocide and mass atrocities, and brought together a list of 15 early warning signs that have been suggested as short- or medium-term predictors. Here I reorder and categorize his list to show the psychological significance of the predictors. I also note how 14 of Verdeja’s 15 predictors apply to the politicide in Rwanda (see Human Rights Watch, 1999, for facts cited below about the Rwanda case).

**Threat Perception**

1. *Public commemorations of past crimes or contentious historical events that exacerbate tensions between groups.* Belgians had used Tutsi to administer their colony; after independence the Hutu-dominated school system taught a history which portrayed Tutsi victimizing Hutu.

2. *Public rallies and popular mobilization against vulnerable groups.* The "Hutu Ten Commandments" were published in a Hutu Power newspaper in Kigali in 1990; the commandments forbade romantic or business relations with Tutsi and demanded that all important positions in Rwanda be held by Hutu.
3. Increased hate media, which may sanction the use of violence against already vulnerable civilian groups. Radio Mille Collines harped on the Tutsi threat represented by RPF incursions from Uganda that began in 1990, and on the Tutsi slaughter of Hutu in neighboring Burundi, calling for attacks on Tutsi both in vengeance and self-defense.

4. Rapid increase in opposition capacity, raising their perceived threat, or conversely a rapid decline in opposition capacity, which may serve as an opportunity to destroy them and their “civilian base”. In February 1993, the RPF showed new strength in a broad advance against the Rwandan army. A truce followed that led to the Arusha Accords and significant political gains for the RPF. Civilians - mostly Hutu - displaced by the fighting streamed south with stories of RPF brutality.

5. Spillover of armed conflict from neighboring countries. Tutsi killed thousands of Hutus in neighboring Burundi in 1972, 1988, and again in 1991. Hutu in Rwanda feared similar treatment by the Tutsi-dominated RPF invading from Uganda. In October 1993, Tutsi officers in Burundi killed Hutu President Ndadaye and thousands died in the ensuing ethnic conflict; Hutu refugees from this conflict living in Rwanda were easily recruited to kill Tutsi.

6. Upcoming elections, which may be perceived as threatening to ruling elites. The Arusha Accords, which called for RPF participation in a transitional government, and for general elections after 22 months, were a direct threat to Hutu elites dependent on the governing party led by President Habyarimana.

Means

7. Increase in weapons transfers to security forces or rebels. In 1993, the Rwandan government and some of its well-to-do supporters bought machetes and small arms for the Interahamwe, a militia organized by the governing Hutu party. On the rebel side, the Ugandan government armed and supported the Tutsi RPF from its first incursion into Rwanda in 1990.

8. Deployment of security forces against previously targeted civilian groups. The Interahamwe were first put to killing Tutsi in Bugesera in March 1992.

9. Nowhere for targeted civilian groups to flee as violence escalates. Once killing began, the Rwandan army set up roadblocks on major roads, and the Interahamwe set up roadblocks on smaller roads to prevent Tutsi from fleeing.

10. Physical segregation or separation of the targeted group from the broader population, forced removal or settlement of populations. Rwandans had government-issued identity papers that specified Hutu or Tutsi beneath their picture - a Tutsi identification card (in practice lack of a Hutu identification card) was a death sentence for those stopped at roadblocks.

Opportunity

11. Natural disasters, which may overstretch already weak state capacity and embolden opposition groups. Beginning in the late 1980s, Rwanda suffered economically from drought as well as a sharp drop in world prices for coffee and tea (Rwanda’s major exports), and from limits on government spending imposed by the World Bank.

12. Rapid change in government leadership, such as through assassination or coup, which can create a power vacuum and result in violent contestation for political power. Rwandan President Habyarimana and Burundian President Ntaryamira, both Hutus, were killed when a surface-to-air missile hit their plane as it prepared to land in Kigali.
13. **Commencement/resumption of armed conflict between government forces and rebels.**
   The RPF resumed its offensive from Uganda, suspended in the ceasefire that led to the Arusha Accords, immediately after President Habyarimana’s plane was shot down.

14. **Arrest, torture, disappearance or killing of political, religious, or economic leaders.**
   The beginning of politicide in Kigali was the targeted assassination of Hutu opposition leaders and their families. Loss of moderate Hutu leaders gave Hutu extremists within the government a free hand to lead fearful Hutu against their Tutsi neighbors.

15. **Sharp increase in repressive state practices, including removal of political, religious, civil and economic rights, stripping of citizenship. Shift from selective to widespread patterns of repression.** From 1975 to 1990, President Habyarimana controlled Rwanda as the leader of a one-party state. In 1990 he was forced to allow competing political parties. Thus, the years immediately before the politicide saw what appeared to be political liberalization rather than increased repression.

The first thing to notice about this list is that the Rwanda politicide was heavily over-determined, with all but one of the 15 warning signs present (all but number 15).

The second thing to notice is the distribution of warning signs across categories - six are signs of increased threat perception, four are signs of increased capacity for killing (means), and five are signs of increased opportunity for killing. Psychological analysis of mass killing usually focuses on motives - why perpetrators and those who direct or support them feel that killing is justified. Indeed, my identification of four kinds of threat that can lead to politicide is just such an analysis of motives. Against the usual focus on motivation, Verdeja’s list is a useful corrective. It reminds us that killing requires not just motives, but also means and opportunity. Particularly for mass killing, means and opportunity are crucial predictors.

**Intervening Against Politicide**

A number of outside actions have been proposed to deter politicide. Suppressing the communications, including radio and TV, of the stronger side is one possibility, economic sanctions are another, and arming the weaker yet another. A more expensive action is direct military intervention to prevent or stop mass killing. It is difficult, however, to muster international agreement to implement such interventions – which is a political problem beyond the scope of this chapter.

In any case, these are interventions based on rational choice theory, specifically deterrence theory. Such interventions aim to present leaders and elites of the stronger side of a conflict with costs that are greater than the perceived benefits of mass killing. But these interventions do not address the emotions behind mass killing: fear, anger, and disgust. Rational choice calculations may not succeed in a competing context of strong emotions.

Perhaps a more promising approach is to dissuade other countries from supporting the stronger side, especially after episodes of killing by category have begun. A success story of this kind is the campaign to brand the 2008 Olympics in China as the “Genocide Olympics” because of China’s support for the Omar al-Bashir government in Khartoum that was fomenting mass killing in the Darfur region of Sudan. To save its Olympics, China reversed its opposition to UN peacekeepers in Darfur and the killing was reduced, if not eliminated.32

It is critical to recognize, however, that outside interventions to dissuade the stronger side from attacking the weaker become much less effective once mass killing has begun. Now the perpetrators of politicide feel the kind of desperation that terrorists feel. They must succeed in eliminating the weaker side or the weaker party will take their revenge. Only a major military intervention can halt mass killing once it has begun.

Some idea of what a major military intervention can mean is provided by the NATO peacekeeping mission in Kosovo (KFOR). In 1999, KFOR entered Kosovo with about 50,000
troops from 39 countries; in 2019 KFOR numbers were still about 3,500 from 28 countries.\(^{33}\) The population of Kosovo is about 1.8 million, so KFOR at its peak strength amounted to about one soldier for every 36 locals. The population of Rwanda is about 12 million - the same 1 to 36 ratios would require about 300,000 soldiers. The implication of this calculation is that, once politicide began in Rwanda, effective intervention from the outside would have required something like 300,000 troops, perhaps 20 divisions. Once violence has begun, peacekeeping is difficult and expensive.

A similar lesson emerges from the UN’s efforts against violence in the DRC. The UN mission, known as MONUSCO, has been in the DRC since 1999. In 2019 the MONUSCO mission numbered about 20,000, including military troops, observers, and civilians. The 2019 UN budget for MONUSCO was over one billion dollars; the total cost to UN donor countries since 1999 has been almost 18 billion dollars.\(^{34}\) MONUSCO casualties up to July 2019 included 176 deaths.\(^{35}\) In sum, MONUSCO has been expensive, in both dollars and lives, in a mission that has lasted over 20 years without putting a serious dent in the mass killing in the DRC.

It is possible to argue that the moral case for UN peacekeeping missions should not be affected by cost, or even by effectiveness. One can say that there is a moral case for \textit{trying} to stop the killing, whatever the effectiveness may be. But no one should doubt that, once mass killing begins, it is difficult and expensive to stop.

\textit{Some Observations about Politicide}

Following the discussion above, it is possible to put together some generalizations emerging from studies of politicide.

1. Politicide is a form of asymmetric conflict, in which the stronger side attacks the weaker.
2. Understanding politicide requires analysis of both sides of the conflict, the weaker as well as the stronger.
3. Perceived threat - including material threat, status threat, security threat, and pollution threat - is an important part of the motivation of mass killing.
4. These threats are associated with strong emotions, including fear, anger, and disgust.
5. Means and opportunity are also important predictors of mass killing.
6. The psychology of support for mass killing appears to be importantly different for perpetrators, leaders, and the mass of those they claim to represent.
7. The actual perpetrators of mass killing are usually few, seldom more than a few percent of adult (largely) males in the stronger group.
8. Individual-level rewards and punishments are often important for recruiting perpetrators.
9. Once begun, mass killing is difficult and expensive to stop.

In the two sections that follow, I begin with these generalizations and offer suggestions toward preventing and ending terrorism.

\textit{From Understanding Politicide to Understanding Terrorism: Looking at Both Sides of the Conflict}

Politicide is mass murder by the powerful side of an asymmetric conflict - the stronger side waging war on the weaker. Terrorism is the warfare of the weak, who is only during an attack locally and temporarily superior to the stronger. Thus, the first conclusion of this chapter is that neither politicide nor terrorism can be understood by looking only at the side of the
perpetrator - every asymmetric conflict has two sides and it is the interaction of the two sides over time that produces the violence of politicide and the violence of terrorism.

For politicide, attention to both sides can be impeded because attention to the weaker side can be seen as blaming the victims. Nevertheless, this attention is necessary for understanding the history of the conflict. It is often a history of threatened or actual status inversion.

Thus, we cannot understand the Armenian politicide without noticing Christian Armenian success in business and education that reversed their low status as a minority group under Muslim Ottoman authority, and noticing as well that many Armenians, including some from Ottoman lands, volunteered to fight with Russian forces against the Turks in the First World War. Similarly, we cannot understand Nazi killing of Jews without noticing Jewish success in business, education and the arts that reversed their low status as a minority in Germany and Austria. We cannot understand Khmer Rouge killing Vietnamese and “Cambodians with Vietnamese minds” without noticing that Vietnam and Cambodia had centuries of conflicts, and that anti-Vietnamese sentiment was high among Cambodians during the US-Vietnam war, including mass killing of ethnic Vietnamese by Lon Nol’s “anti-Communist” forces. We cannot understand Hutu killing Tutsi without noticing how the Belgians had used the Tutsi minority to control the Hutu majority in Rwanda, and without noticing as well the Tutsi killing of Hutu to maintain control of a Hutu majority in neighboring Burundi.

In short, normal human beings are usually not eager to engage in mass killing. Few want to work in a slaughterhouse; killing and the results of killing are disgusting. There is always a history of intergroup conflict, often a history of threatened or actual status reversal, that is used to justify mass killing.

Like politicide, insurgent terrorism is a form of asymmetric conflict, and the same conclusion applies: terrorism cannot be understood without looking at both sides of the conflict. Terrorists are the weak attacking the strong, a non-state force challenging the power of a state. In this case, it can be difficult to attend to the actions of the state and its citizens, because again to do so seems to be blaming the victims. Nevertheless, this attention is necessary for understanding the history and evolution of the conflict from which terrorism emerges. It is often a history of threatened or actual status inversion.

Thus, we cannot understand Islamist terrorism without noticing the grievances of many Muslims against Western countries, especially against the US. These grievances are a familiar litany to scholars of terrorism but not always obvious to government security officials and the citizens of Western countries. A prominent form of grievance is Western support for authoritarian governments in predominantly Muslim countries. Muslims point to the speed with which Western governments in 1991 recognized a military coup against an Islamist election victory in Algeria, and similarly recognized the military coup against an elected Islamist government in Egypt in 2013.

Another prominent grievance is the presence of US troops in predominantly Muslim countries, including 14 Middle Eastern and North African countries. US military operations in these countries bring civilian casualties - collateral damage - that can appear frequently in horrifying internet videos. A long-term grievance is continuing US support for Israel in its conflicts with Palestinians and neighboring Muslim countries.

These grievances can be understood as including material, status, and security threats to Muslims. Some Muslims also feel a contamination threat as Western individualist, corporate culture moves into Muslim economies and media streams. We do not need to agree with these grievances to recognize that they are part of the conflict and part of what moves some Muslims to justify or engage in terrorism.

Similarly, we cannot understand right-wing terrorism in the US without noticing the grievances of blue-collar (largely) white Americans. Economically, their wages have stagnated - even two-earner families can barely keep up. Culturally, they have been diminished in a global, information-based, status order that depends on elite education. Even as they are
diminished economically and culturally, they see the agencies of government, especially the federal government, supporting the rise of immigrants, refugees, LGBT groups, white-collar government workers, and international corporations.

Opposition to immigrants and refugees in particular is expressed in the slogan “You Will Not Replace Us” (prominent in the Unite the Right rally, Charlottesville, VA, August 2017). At least in the United States “Replacement Theory” has a certain basis in fact; white Americans are in fact being demographically replaced by minorities. In 2018, non-Hispanic whites were for the first time less than half the US population under the age of 15. Non-Hispanic whites are expected to become a minority of the US population in 2045.

To sum up, perpetrators of terrorism are like perpetrators of politicide: both see threats to their group that are used to justify killing enemy civilians. We do not have to accept that the threats are real to acknowledge that the threats look real to them.

**From Understanding Politicide to Understanding Terrorism: Looking Separately at Leaders, Perpetrators, and the Mass of Those They Claim to Represent**

Mass killing requires a substantial organization. It follows that there are usually big differences between the top of the organization and the bottom, between leaders and perpetrators of violence. The differences are even greater when the perpetrators of mass killing are part of a military or paramilitary organization. Some of these differences are obvious. Leaders order killings but seldom carry out any violence themselves (except perhaps suicide, like Hitler, if the enemy is winning). Leaders face an enemy threat different from perpetrators: loss of status and power if the enemy wins. Leaders are usually older and better educated than perpetrators. These differences are less likely in a terrorist group, which is often so small that leaders share the same life and the same risks as other group members. Status and demographic differences are likely to be smaller in a terrorist group, and leadership is likely to depend more on personal relations and group dynamics than on the authority of official ranks. Importantly, leaders in a small terrorist group usually also take part in armed combat. Thus, in a small terrorist group, the distinction between leader and perpetrating followers becomes small, sometimes near to vanishing. This was the case for 1970s leftist terrorists in the US, Italy and Germany (Weather Underground, Red Brigades, Red Army Faction respectively), most of whom had some university education.

Of course, there are larger terrorist groups in which leaders and perpetrators are very different people. Shining Path in Peru was founded and led by a philosophy professor, whereas most of the perpetrators of violence were recruited from rural youth. The Irish Republican Army (IRA) had commanders and “active-service volunteers” in an explicitly military model. In larger terrorist groups, there are specializations that distinguish not just leaders and perpetrators, but organizational roles such as intelligence, bomb-making, logistics, finance, and public relations. Despite the differences resulting from group size, there are basically two ways to become a member of a terrorist group. The first way is to volunteer to join an existing terrorist group. This was the case for individuals traveling to Iraq and Syria to join Islamic State, or to Somalia to join al-Shabaab. The second way is a gradual escalation of radicalization and violence as a terrorist group spins off from some larger movement or protest group. This was the case for many of the 1970s leftist terrorist groups, which spun off as the extremes of university-based anti-war protest groups (e.g. the Weather underground in the US).

Looking at terrorist case histories from different continents and centuries, McCauley and Moskalenko identified three mechanisms of group dynamics that can move a whole group to terrorism. The three mechanisms of group dynamics are extremity shift after group discussion among like-minded individuals, radicalization from intergroup competition, and the multiplication of these two dynamics that comes from group isolation. These three mechanisms
help explain how a whole group can move together from protest to terrorism, as occurred with 1970s leftist terrorist groups.

Turning now to those who volunteer for an existing terrorist group, McCauley and Moskalenko identified six individual-level mechanisms of radicalization. The obvious one is group grievance, as already described. The other mechanisms include personal grievance (“they mistreated me or mine”), love for someone already in the terrorist group, slippery slope (slow escalation of support for the group to the point of joining), risk and status seeking, and escape from personal problems, including loneliness.

Except for group grievances, the individual mechanisms depend more on self-interest than group interest. Indeed, these mechanisms show considerable overlap with the self-interested motives mentioned in relation to joining in mass killing. To repeat, some join out of habitual obedience to authority and fear of punishment if they don’t join. Some join for the status and power of having a gun in their hands. Some join for salary or loot, for access to alcohol and rape, for comradeship, or to escape problems at home or with the law.”

It is encouraging to see this convergence of research on perpetrators of politicide and research on perpetrators of terrorism. Both do violence for a group cause, but more self-interested motives appear important for both kinds of perpetrators. Most individuals who join a terrorist group will learn the group’s rationale of grievance after joining, but, as with politicide, grievance and group threat cannot explain why perpetrators are few compared with the many who share the grievance.

What about the mass of those who are neither leaders nor perpetrators of violence? Here is where terrorism research has better data than politicide research. Leaders and perpetrators of politicide claim to represent the whole of the stronger side, but mass opinion is largely unknown. How many justify the violence of politicide is difficult to ascertain; polling of the stronger side before and during politicide is not available. But polling of the group supposedly represented by terrorist leaders and perpetrators is often available.

McCauley reviewed opinion polls of US and European Muslims since the 9/11 attacks. Contrary to those who cite discrimination against Muslims in Western countries as the source of terrorist attacks from among these Muslims, poll results consistently showed the importance of Western foreign policies. In round numbers, about 40 percent of Western Muslims feel that the war on terrorism is a war on Islam. About ten percent say that suicide bombing against civilians is often or sometimes justified in defense of Islam.

These are the ideas that must be targeted in the war of ideas against Islamist terrorism. Broadly held Muslim sympathies for terrorist causes, and justifications of suicide bombing, are what allow a few gullible young Muslims among them in the West to feel that violence will move them “from zero to hero.” To target these ideas, it is necessary first to recognize their importance.

Similarly, for right-wing terrorism, polling data can tell us about the many sympathizers and supporters who themselves are not involved in violence. Here is a poll item that taps sentiment toward immigrants: “Do you think the number of immigrants from foreign countries who are permitted to come to the United States to live should be increased a little, increased a lot, decreased a little, decreased a lot, or left the same as it is now?” Respondents saying decreased a little or a lot were coded as anti-immigrant, and results for 2008 showed that the anti-immigrant percentage ranged from 63 percent in Arizona to 34 percent in California.

Evidently there is broad and substantial support in the US for the right-wing antipathy to immigrants. The slogan “You will not replace us” is likely to have increased appeal as more citizens learn what demographers and right-wing terrorists already know: non-Hispanic whites will soon be a minority in the US.

The next section discusses what can be done to counter terrorism after recognizing that terrorists, like mass killers in politicide, have grievances that cannot be suppressed or ignored.
From Understanding Politicide to Understanding Terrorism: Countering Political Violence and Terrorism

An old adage has it that “an ounce of prevention is worth a pound of cure.” Recognizing grievances before terrorism begins can be the ounce of prevention.

Few groups move to terrorism as their first political expression. Peru’s Shining Path came close to this kind of start; it spent nearly a decade recruiting quietly in rural areas before its first terrorist attack in 1980. But the usual pattern is a longer period of escalating protest, activism, attacks on property, and attacks on security forces and government officials before moving to attacks on civilians. This was the trajectory of 1970s student-based movements in the US, Italy, and Germany that protested against the Vietnam War.

The time to prevent terrorism is early in the escalation of intergroup conflict. In her history of Italy’s Red Brigade and Germany’s Red Army Faction, Della Porta emphasized the escalation of violence between police and protesters. With each escalation, some protesters gave up radical action but others, outraged by their own injuries and arrests or those of their friends, escalated their violence against police and government officials.

The first step in avoiding escalation is treating protesters with restraint and careful observance of their rights as citizens. And the foundation for restraint is recognizing protester grievances. Rather than treating protesters as traitors or ‘crazies’, authorities should treat them as citizens with a grievance they are entitled to express. This can be difficult when protesters are insulting the police, spitting at them, making fun of them. But difficult is not impossible.

Sometimes, as in authoritarian states, protests can be crushed, but in most Western countries, norms of rule of law and procedural justice will generate new sympathy and new recruits for protesters who are suppressed. The most successful recruitment tool for the IRA was Bloody Sunday, when British soldiers shot 26 unarmed Irish civilians participating in a protest march.

The War of Ideas against terrorism should begin before, not after, the first terrorist attack. A social movement or political movement that attacks particular government policies - or after escalation, attacks the legitimacy of an entire government - can be countered in one of two ways.

The first and most obvious, the default response to those who challenge government policies, is to defend these policies. The protesters are wrong, the government is right. The protesters are victims of propaganda and misinformation.

Thus, the US reaction to Islamist extremism has been attacks on Islamist groups. The US State Department’s “Think Again, Turn Away” program, initiated in English in 2013, seems to have tweeted more about what’s wrong with ISIS and its supposedly idyllic state than about what’s right about US foreign policy. Google’s Redirect program, which began in 2016, sends users seeking Islamic-State-related content to anti-ISIS YouTube videos.

Reaction to right-wing extremism has been similar. In 2019, Facebook initiated a ban on “white nationalist” and “white supremacist” content. Users seeking or posting such content will be directed to a nonprofit group’s website that aims to help people leave hate groups.

The reaction to both Islamist and right-wing extremism have this in common: to try to suppress extremist messages and show the negative sides of extremist groups. Notably absent is anything like an explicit rebuttal of extremist grievances; there has been no defense of US foreign policy in Muslim lands, no argument why white decline in Western countries is not a threat.

Unfortunately, it does not appear that suppression and denial are working. It has been 19 years since the attacks of September 11, 2001. The US military, as already noted, is involved in fighting terrorism in numerous, predominantly Muslim, countries. Trillions of dollars have been spent on the war on terrorism and for US homeland security. But Western Muslims were still trying to join Islamic State until it was vanquished as a military force in 2018-2019. A
trickle of Muslims, mostly second and third generation immigrants, continue to attempt terrorist attacks in North America and Northern Europe.

In short, the War of Ideas is not working. So long as 40 percent of Western Muslims see the war on terrorism as a war on Islam, so long as ten percent justify suicide bombing in defense of Islam, so long will a few individuals and small groups rise in what they understand as retributive and liberating violence.

A second and more promising approach to the War of Ideas against Islamist terrorism is to admit that Muslims have real grievances and move the argument to whether violence is a useful response to these grievances. This approach can be found in the UK. Deradicalization (de-rad) of individuals convicted of terrorist offenses in the UK is in the hands of probation officers, often working with community groups that try to provide support and mentoring for probationers. Sara Marsden has interviewed more than 30 of these frontline de-rad workers to learn what they do and what they think works. The results are interview excerpts rather than statistics about success and failure.

The radicalizing issue for many probationers is foreign policy. Here is a senior probation officer talking:

“Social exclusion, racism, things like that, you know, diversity’s a big part of it, foreign policy, perceived injustice, and grievance... grievance is an important part, foreign policy, it’s about the impact factors, that people are seeing Muslim children dying on the TV, these can have big impacts on people”.

A notable finding of the interviews Marsden conducted is that probation officers and community mentors report some success with interventions that do not directly challenge jihadist ideas. Instead, interventions aim for disengagement and desistance by debating not the grievance, but the violent response to grievance. Here is a community mentor talking:

“…. if they want to talk about foreign policy, we’ll just join their argument, you know, I think you’re right about Afghanistan or Iraq, why should other people go into Afghanistan or Iraq and kill innocent people, they’ve no right to go there - yes, you’re right. So, then these people start thinking, well hang on we’ve got the same views, at the end then, when the conversation finishes on that particular subject, what we have both agreed is that, yes, we don’t like it what’s happening, but what is the action we can take, to stop that from happening?”

This kind of intervention may be particularly helpful with individuals who strongly empathize with the suffering of others. Rather than insist the probationer deny Western victimization of Muslims, or deny that this suffering justifies violence in return, the debate turns on whether violence or support for violence is the most effective response to Muslim grievances. Here, a probation officer reflects on the limits of the possible in deradicalization:

“He’s always going to have strong political beliefs, that’s the way he is, and he’s got a really strong sense of injustice, but I think what he’s learned now, is that he can’t channel those in the way he was.”

It seems that UK probation officers have discovered a way to get beyond the suppression and denial that is not working in the War of Ideas against Islamist terrorism. Something similar may be useful against right-wing terrorism in the US. Consider the attack targeting Hispanics
in El Paso, Texas, on 3 July 2019. The attack killed 22 persons and injured 24 others. The killer left a manifesto citing the “Great Replacement,” to say that he was defending against foreign invasion. The response of many US politicians has been to say that the attack is “senseless” (tantamount to saying the perpetrator is crazy), that white people are far from disappearing, that Americans should remember that the US has always been an immigrant nation.\textsuperscript{52} Public response to the attack has featured marches against hate.

None of these reactions speak to those who are feeling fear and anger about the status decline of white Americans. It is not useful to tell those in the grip of strong emotion that they are mistaken, that there is nothing to fear, nothing to be angry about. A more useful approach might be to acknowledge the ongoing apprehension among many white Americans or a demographic replacement and then ask what might usefully be done about this perceived threat. Is violence going to help? Are other responses possible? What might be done to improve the social and economic welfare of blue-collar workers in the US? Might such improvement raise the birthrate of blue-collar families, including white families?

These particular possibilities are not crucial; it is a response that starts from acknowledgment of grievances that is important. As in the case of Islamic grievances, public recognition of white nationalist grievances might do more against radicalization than suppressing and denying the existence of such grievances. Suppressing and denying grievances tends to create anger and alienation on top of the original grievances, in this and other cases.

\textbf{Conclusion}

Politicide and terrorism are related as outcomes of asymmetric conflict that has escalated to violence. Most intergroup conflicts do not evolve to violence, but to understand those that do we need to consider both politicide and terrorism as forms of intergroup conflict. Theory and practice require specifying the conditions under which asymmetric conflict leads to violence. Perceived threat, means, and opportunity are all potential predictors of both politicide and terrorism.

For groups with more power, there are four kinds of threat: material, status, security, and pollution threats. Material threat instigates mostly anger; status threat instigates both anger and shame; security threat instigates fear; and pollution threat instigates disgust. The 9/11 attacks, for instance, combined material, status, security, and security threats to the US.

Although many believe that the predominant response to terrorist attack is fear, there is evidence that anger is predominant. Back, Küfner, and Egloff examined emotion words in millions of words of texts sent in the US on the day of the 9/11 attacks.\textsuperscript{53} Anger-related words increased throughout the day, ending six times higher than fear- and sadness-related words. This result is important for two reasons. First it shows the usefulness of assessing mass opinion, especially emotions, for the victims of terrorist attacks. Mass opinion can be of interest not only for terrorist sympathizers but also for terrorist victims. Second, it warns of the power of \textit{jujitsu politics}, the terrorist strategy that aims for anger and over-reaction that is likely to increase sympathy and recruitment for the terrorist cause.\textsuperscript{54}

For groups with less power, the same four threats have become reality in four different kinds of perceived loss. Material loss instigates anger; status loss instigates anger and shame; cultural identity loss instigates fear; and too many of them contaminating “us” instigates disgust. An important difference between politicide and terrorism, then, is the difference between threatened loss and actual loss. The four threats that move the more powerful towards the use of violence against the less powerful are usually threats of anticipated loss with relatively small actual losses. In contrast, the less powerful side attacks the more powerful with a sense of desperation that comes from experiencing the four threats as having become the reality of four kinds of major losses.
Both politicide and terrorism are extreme forms of violence that target civilians. Extreme violence is almost always preceded by lesser forms of violence, including violence against property, violence that does not necessarily cause irreversible harm (beatings, rape, torture, expulsion), and killing on a smaller scale before larger killing. Escalation of violence usually includes an expansion of the category of acceptable targets. This expansion has both a moral and a cognitive aspect. Morally, escalation means that more of ‘them’ are seen as guilty of, or supportive of, violence against ‘us’; thus, more are justifiable targets of our justice, revenge, and self-defense. Cognitively, escalation means that they are essentialized such that “they are all the same,” “they are disgusting.” Therefore, all of them are justifiable targets. This is the significance of calling the enemy by the names of disgusting life forms - viruses, lice, cockroaches, rats, and pigs, for example.

To sum up, studies of politicide lead to three generalizations relevant to countering terrorism.

First, neither politicide nor terrorism can be understood without studying both sides of the conflict. Rather than studying only the perpetrators of violence, the victims must also be studied. An impediment to this kind of study is that it risks blaming the victims. Studying the victim group in mass killing, or the victim group in terrorist attack, is nevertheless required to understand the trajectory of intergroup conflict that produces violence against civilians. For both politicide and terrorism, trajectories of escalating violence depend on means and opportunity. Politicide requires the identification of victims, means of killing, and organization and motivation of killers. When politicide has the power of a state behind it, the means and opportunity are not difficult to find. For terrorists, without the power of a state, the means and opportunity are more problematic. But terrorists still require the identification of victims, means of killing, and organization and motivation of killers. These requirements have led security officials to focus on terrorist attempts to surveil targets, procure firearms and bomb materials, and communicate grievances and methods on the internet.

It is worth noting that means and opportunity can create motivation. An example is the case of Dr. al-Balawi, whose suicide bombing at Khost in December 2009 killed several high-level CIA agents. Months of internet flaming in support of jihad and suicide bombing did not lead al-Balawi to any radical action. Then Jordanian intelligence officers forced him to travel to Pakistan to try to make contact with Dr al-Zawahiri. Connection with jihadist militants provided means and opportunity and al-Balawi moved from radical opinion to radical action. Al-Balawi wrote that he would be ashamed not to take up the bomb vest once it was offered.55

Second, neither politicide nor terrorism can be understood without separate attention to leaders, perpetrators, and mass sympathizers of violence against civilians. The differences between leaders and perpetrators tends to be larger for politicide than for terrorism. Nevertheless, perpetrators of politicide and terrorism are similar in the importance of individual and selfish motives in recruitment to violence. Perpetrators of both politicide and terrorism are few - usually just a few percent - in relation to the size of the group they claim to do violence for. The outgroup threat in asymmetric conflict is felt by many on both sides, and cannot explain why so few engage in violence. Individual and selfish motives, and means and opportunity help explain the perpetrators’ action.

Assessment of mass opinion is an important part of understanding asymmetric conflict. As politicide and terrorism are forms of political conflict, the everyday tools for the analysis of political competition will be useful - not just polling but focus groups, and careful pilot testing of new messages and policies.

Polling before and during politicide is difficult, but polling to understand terrorism is not. Polling of both terrorist sympathizers and terrorist victims is relatively easy and often available. The first can track progress in the War of Ideas; the second can track the success of the terrorist strategy of seeking over-reaction to terrorist attack (jujitsu politics).
Third, interventions against politicide and terrorism require recognizing the intergroup threats and grievances perceived by both stronger and weaker sides of the conflict. Like the weaker side, the stronger side in politicide perceives threats and feels grievances. These are the justification of mass killing; if they seem unreal to outsiders, they are nonetheless real to the killers, their leaders, and at least some of those they claim to represent. Likewise, terrorists perceive threats - and losses - perpetrated by the state they oppose.

Interventions against terrorism are unlikely to succeed without attention to the threats and grievances perceived by terrorists and their sympathizers and supporters. For Islamist terrorism, this means attention to grievances relating to Western foreign policies toward predominantly Muslim countries. Instead, Western governments have focused on what’s wrong with jihadist groups and their fundamentalist forms of Islam, and have tried to suppress or ignore Muslim grievances. So far there is no sign that suppressing and ignoring grievances shared by substantial percentages of Muslims, including Western Muslims, is winning the War of Ideas.

UK counter-radicalization practitioners have discovered a promising and constructive alternative to suppressing and ignoring; they agree that Muslims have real grievances against Western foreign policies, then turn the discussion to how best to reduce these grievances. The human and moral costs of violence are easier arguments than convincing Muslim activists and terrorists that Muslim grievances are illusory.

Similarly, for right-wing terrorism, interventions are unlikely to succeed without attention to the threats and grievances perceived by terrorists and their sympathizers. This means, in the case of the US, attention to genuine grievances relating to the status decline of non-Hispanic whites in relation to darker-skinned immigrants. Instead, Western governments have focused on what’s wrong with right-wing groups and with right-wing terrorist individuals. Labeling right-wing terrorists as mentally unstable racists does not address the anti-immigrant sentiments shared by millions of Americans and by many Europeans as well.

Politicide and terrorism emerge out of asymmetric conflicts - political conflicts with histories of action and reaction over time. It is these trajectories of conflict that must be understood to prevent and reduce the extremes of violence against civilians that are justified as “killing them to save us.” Finding, fixing, and finishing the individual perpetrators of violence against civilians, few as they are - at least in the West - will not resolve the problem.

Clark McCauley is Research Professor of Psychology at Bryn Mawr College. His research interests include stereotypes, group dynamics, and the psychological foundations of ethnic conflict and genocide. He is co-author of “Why Not Kill Them All? The Logic and Prevention of Mass Political Murder” (2006), co-author of “Friction: How Radicalization Happens to Them and Us” (2011, second edition 2017), co-author of “The Marvel of Martyrdom: The Power of Self-Sacrifice in a Selfish World” (2018). Dr. McCauley is founding editor emeritus of the journal “Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide”. He is also a lead investigator with the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland.
Endnotes


6. Emphasis added CM.


Frey, William H., ‘Less than half of US children under 15 are white, census shows.’ 

41 Ibid., pp. 13-94.
45 Katz, Rita, ‘The State Department’s Twitter War with ISIS Is Embarrassing,’ Time, 16 September 2014. Available at: https://time.com/3387065/isis-twitter-war-state-department/.
50 Marsden 2017, p. 63.
51 Ibid., p. 100.
54 McCauley and Moskalenko 2017 pp. 149-160.


Frey, William H., ‘Less than half of US children under 15 are white, census shows,’ Brookings, 2019. Available at: https://www.brookings.edu/research/less-than-half-of-us-children-under-15-are-white-census-shows/


Katz, Rita, ‘The State Department’s Twitter War with ISIS Is Embarrassing,’ *Time*, 16 September 2014. Available at: https://time.com/3387065/isis-twitter-war-state-department/.


McCauley, Clarke, ‘Constructing Terrorism: From Fear and Coercion to Anger and Jujitsu


United Nations Peacekeeping, Fatalities by mission and appointment type, up to 31 Jul 2019. United Nations Peacekeeping, 2019. Available at:
Web-based Resources

Academia, Academia.edu
Bryanmawr College, https://www.brynmawr.edu/people/clark-r-mccauley
Google Scholar, https://scholar.google.com
National Consortium for the Study of Terrorism and Responses to Terrorism (START),
https://start.umd.edu
Research Gate, https://www.researchgate.net/profile/Sophia_Moskalenko
Research Gate, https://www.researchgate.net/profile/Clark_Mccauley
Chapter 7

At the Crossroads: Rethinking the Role of Education in Preventing and Countering Violent Extremism

Thomas K. Samuel

This chapter looks at the issue of violent extremists and terrorists targeting the education sector, and subsequently recommends steps that the education sector can take to prevent and counter violent extremism (PCVE) amongst students. Educational institutions in general and students in particular have been targeted by violent extremists and terrorists. Paradoxically, they have sought to physically attack and destroy institutions of learning, while at times, they have actively sought to radicalize and subsequently recruit students to join their cause. Short case studies of attacks on educational institutions in different parts of the world, as well as instances of young people being radicalized in schools and universities, are presented and evaluated. Emphasis is then put on revisiting the idea of education and envisioning a greater role for it to play in PCVE among students. A case is presented for the education sector to take the lead in PCVE among the youth; given education’s strategic advantages in terms of coverage in reaching the youth, duration of contact with the youth, and access into the cognitive and emotional makeup of the youth. A “whole-of-education” approach is proposed, whereby the educational institutes will identify specific areas of the students’ cognitive and emotional spheres in which to build PCVE related “firewalls” in a systematic and comprehensive manner. In this proposed PCVE approach, teachers will take a redesigned role that would focus more on mentoring and guiding, preparing a “safe space” to initiate discussions, and building trust and credibility to maximize their ability to impart the contents to the students. Additionally, given the complexities involved in reaching out to the youth on the subject of PCVE, the role of the teachers would be augmented by leveraging on the skill-set, experience, appeal, and support of “select” individuals such as rehabilitated terrorists, former victims of terrorism, social media influencers, and role models.

Keywords: counterterrorism, preventing and countering violent extremism, PCVE, education, children, terrorist attacks, radicalization, schools
Education is powerful.

This has been recognized not only by governments and societies but also extremist and violent organizations. Given this, the education sector has always been the “battleground” for political, religious, and ideological movements, including violent extremist and terrorist groups, to impose their views and values on society. Such groups infiltrate the education sector to manipulate and recruit based on core human identities such as ethnicity, religion, race, and gender. They actively propagate rigid and extreme interpretations of religion and culture to help fashion an intolerant and violent environment for young and impressionable target audiences. Hence, educational institutes are seen as a potential target that offers under one roof thousands of potential recruits for indoctrination and recruitment into violent extremism and terrorism.

Governments and authorities are beginning to recognize this vulnerability in educational institutes and are attempting to “plug the holes” and prevent such institutions from becoming the breeding ground of violent extremism. Whilst this is undoubtedly necessary, the authorities would be missing a golden opportunity should they not realize that not only are educational institutions vulnerable to violent extremism but ironically, given the right support, they have the potential of becoming citadels for preventing and countering violent extremism (PCVE) among the youth. Simply put, schools and universities can move from being possible breeding grounds for potential sympathisers and recruits to instead active PCVE. This chapter will argue that the best defense against extremist ideologies taking over institutions of learning is to develop an education system that will prepare and equip the students to debate and defeat extremist thoughts.

**Scope, Parameters and Definitions**

This chapter will firstly consider the state of vulnerability of students in educational institutes towards violent extremism by looking at case studies, as well as the literature on the subject. Secondly, the possible interventions, via education, in preventing and countering the trajectory into terrorism will be discussed. The institutions of learning that are covered in this chapter include public schools and universities, but will exclude religious or faith-based educational institutions.

I am mindful of the wiry observations of Schmid and Jongman that “authors have spilled almost as much ink [while trying to define the concept of terrorism] as the actors of terrorism have spilled blood,” and would therefore borrow Resolution 49/60 which the UN adopted during the General Assembly. It defines terrorism as “criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes.”

Shifting from defining “terrorism” to “violent extremism,” like the proverbial moving from the “frying pan into the fire,” is fraught with challenges. The Federal Bureau of Investigations defines violent extremism as “encouraging, condoning, justifying, or supporting the commission of a violent act to achieve political, ideological, religious, social or economic goals.” The United Nations Plan of Action to Prevent Violent Extremism observed that “violent extremism is a diverse phenomenon,” admitting that it was “without clear definition” while acknowledging that it “encompasses a wider category of manifestations” when compared to terrorism. Finally, in the context of this chapter, radicalization refers to the pathway or process that mobilizes a (young) person to support and ultimately engage in acts of political violence.
Education as a Target

The targeting of education in general, and institutions of learning in particular, by violent extremists is not a new phenomenon. Political entrepreneurs and agitators have always viewed educational institutions as recruiting grounds, but also as a potential threat to their ideologies. The persecution of Arab and Jewish scholars in Spain during the 15th century, the suppression of Jewish and socialist intellectuals by the Nazis in Germany, and the mass targeted killings of scholars by the Khmer Rouge in Cambodia are but a few examples in history.\(^6\)

In 2010, UNESCO published a detailed study that looked at political and military violence against the whole spectrum of the education system worldwide.\(^7\) The report highlights that possible motives for such attacks include:

- targeting what was perceived to be symbols of the imposition of an alien curriculum, value, culture, philosophy, or ethnic identity;
- preventing the education of girls;
- preventing any form of education;
- targeting what was seen to be symbols of government power and one of the most visible symbols of state authority;
- undermining the confidence in government authority over a particular area;
- extracting revenge for civilian killings;
- undermining the functioning of the education system;
- abduction of children and at times adults, with the intent of recruiting them to provide forced labour, sexual services and/or logistical support;
- abductions for ransom;
- sexual violence by members of armed groups, soldiers or security forces as a tactic of war or out of disrespect for gender rights;
- attacking students and academics with the intent to silence political opposition or prevent the voicing of alternative views;
- attacking students and academics to specifically silence human rights campaigns;
- attacking academics to limit research on sensitive topics; and
- destruction of education institutions by invading forces as a tactic of defeating the enemy and destroying education buildings in revenge.\(^8\)

Additional motivations identified in the UNESCO study include media coverage that can be generated for the violent extremist groups as a result of an attack on an institution of learning as well as the ease of causing extensive damage to what are usually only lightly defended or totally unprotected targets affiliated with the government.\(^9\)

Research indicates that there has been a rise in attacks on education in recent years. In 2018, the Global Coalition to Protect Education from Attack (GCPEA) published a study\(^10\) that was built on two previous studies published by UNESCO in 2007 and 2010 as well as a third study published by the GCPEA in 2014. The authors of the studies compared global patterns of attacks on education during the 2013-2017 period to those perpetrated earlier, and noted that there appears to be an increase in attacks worldwide. Here are some examples:

Past Attacks on Educational Institutions

Beslan School (Russia)

On 1 September 2004, armed Chechen rebels took approximately 1,200 children and adults hostage at School Number One in Beslan, North Ossetia, Russia. The hostage takers were
members of the Chechen group called the Riyad as-Saliheen Martyrs’ Brigade, which had been founded and led by Chechen warlord Shamil Basayev. The hostage takers demanded the recognition of Chechnya’s independence from Russia and the immediate withdrawal of Russian troops from the region. On 3 September 2004, the Russian security forces stormed the building with tanks, incendiary rockets and other heavy weapons. At the end of the siege, 334 people, 186 of them children, were killed.

**Garissa University College (Kenya)**

On 2 April 2015, Al-Shabaab militants attacked the university in Garissa, Kenya, taking 700 undergraduates as hostages. In the end, they killed 148 people (142 of them students) and injured another 79. Two days after the attack, Al-Shabaab issued a statement threatening Kenyan citizens with “another bloodbath” saying that they would “stop at nothing to avenge the death of (their) Muslim brothers” until and unless the Kenyan government “cease its operations” - likely referring to the Kenyan army’s participation in the African Union’s mission in Somalia against the group. They also warned the Kenyan public that they would be targeting “schools, universities, workplaces and even homes” for “condoning your government’s oppressive policies by failing to speak out against them” and for “reinforcing their policies by electing them.” It is also significant to note that as a consequence of the attack, 96 out of a total of 150 primary and secondary schools were closed in Garissa county due to “security fears” among both students and teachers.

**Army Public School (Pakistan)**

On 16 December 2014, fighters linked to the Tehrik-i-Taliban (TTP) attacked the Army Public School in Peshawar, North western Pakistan. Armed with automatic weapons and grenades and wearing explosive belts, they entered the school by scaling a wall and then proceeded to go from one classroom to the next, opening fire indiscriminately on the school children. In total, the fighters killed 149 individuals of which 132 were students, with ages ranging from eight to 18. A military spokesperson highlighted the fact that all terrorists wore suicide vests, were heavily armed, made no demands, and were also stocked with rations indicated that they did not come to take any hostages. According to retired general and security analyst Talat Masood, the militants were very much aware that they did not have the capacity to “strike at the heart of the military” and therefore chose to go after soft targets, such as the school where most children were from military families. This was calculated to cause a great psychological impact. Justifying the attack, the TTP spokesman Muhammad Omar Khorasani was reported to have said, “we targeted the school because the army targets our families. We want them to feel our pain.” The Peshawar school attack was called the “massacre of the innocents” and the incident was seen as “Pakistan’s 9/11 moment.”

**The Chibok Schoolgirls (Nigeria)**

On 14 April 2014, Boko Haram kidnapped 276 female students who had gone to take exams from a government secondary school for girls in the town of Chibok, Borno State, Nigeria. During the assault, 57 girls managed to jump and escape from the trucks in which they were being driven away. The remaining 219 girls were abducted by the kidnappers. Boko Haram leader Abubakar Shekau reportedly said that all the girls that had been taken had converted to
Islam and had been “married off.” As of March 2020, out of the 276 girls who were kidnapped, 103 girls were released, reportedly in exchange for ransom money and prisoners and four girls were said to have escaped later on their own. There remain another 112 girls unaccounted for. One of the girls who had escaped reported that during the early stages of the kidnapping, the militants had told the girls, “you’re only coming to school for prostitution. Boko (Western education) is haram (forbidden) so what are you doing in school?” The Chibok kidnappings raised international awareness about the atrocities of Boko Haram in Nigeria but did little to stem the flow of more kidnappings as witnessed by the abduction of the 300 elementary school children in Damasak and the kidnapping of the 110 boarding school girls in Dapchi. In April 2018, UNICEF highlighted that since 2013, Boko Haram had kidnapped more than 1,000 children in Nigeria. The UN agency appealed for an end to attacks on schools in Nigeria and said that young girls in particular were especially vulnerable to attacks by the militant group and had been “consistently targeted and exposed to brutal violence in their schools.” UNICEF Nigeria went on to stress that the “repeated attacks against children in schools (were) unconscionable.” UNICEF reiterated that “children have the right to education and protection, and the classroom must be a place where they are safe from harm.”

**Bacha Khan University (Pakistan)**

On 20 January 2016, four gunmen opened fire at the Bacha Khan University in Charsadda, Pakistan, killing 21 people. The four terrorists scaled the walls of the university and then opened fire on students and teachers. A few days before the attack, the authorities had closed some schools in Peshawar as they had reason to believe that an attack was imminent. Charadda is less than 40 kilometres away from Peshawar, where on 16 December 2014, fighters linked with the TTP attacked the Army Public School. In a follow-up video, Umar Mansoor, a Pakistani Taliban spokesman, vowed to target schools throughout Pakistan. He elaborated that his fighters had attacked the university “because this is the place where lawyers are made, this is the place that produces military officers, this is the place that produces members of the parliament, all of whom challenge Allah’s sovereignty.” He went to say that instead of targeting the armed “enemy” soldiers, his group would now change their focus and “target the nurseries that produce such people” and warned that, together with his fighters, “we will continue to attack schools, colleges and universities across Pakistan as these are the foundations that produce apostates. We will target and demolish the foundations.”

**Susceptibility of the Youth to Radicalization**

Young people between the ages of 15 and 25 are vulnerable to following extremist ideologies as they are at a developmental age where they are searching to discover their own identities, bolster their self-confidence, and find meaning in their lives. This age group is also quite action-orientated and young people are oftentimes characterized as being more prone to taking greater risks. Their minds are also more susceptible to external influences than those who are more experienced, and therefore they have fewer built-in “safe-guards” against extremism. Hence, for youth, the limited ability to compare belief systems and the lack of capacity of many to view things other than black or white, translates to the premise that a “radical ideology does not seem radical at all.” This susceptibility is well recognized by violent extremists and, consequently, this vulnerability is very much exploited.
**Terrorist Recruits Getting Younger?**

Young people serve as a vital source of support for terrorist groups. In Sri Lanka, the Liberation Tamil Tigers of Elam (LTTE) have actively recruited children into their ranks. Tamil children were said to have been targeted for recruitment from age 11. The LTTE was reported to “routinely visit Tamil homes to inform parents that they must provide a child for the movement.” Parents were bullied and threatened to comply with the LTTE’s request of forced conscription of their children. Children were at the onset recruited into the LTTE’s “Baby Brigade” but later integrated into other units. For example, the elite “Leopard Brigade” was said to have been formed from children taken from LTTE-run orphanages; it allegedly became one of LTTE’s fiercest fighting units. In 1991, a major LTTE military operation against the Elephant Pass military complex was said to have used waves of children drawn from the “Baby Brigade.” The operation resulted in an estimated 550 deaths of LTTE members, the majority of them being children. There were also reports that 40 to 60 percent of the LTTE soldiers killed during the conflict in the 1990’s were children under the age of eighteen. Children were also allegedly used for “massed frontal attacks” in major battles. Those between the ages of twelve and fourteen were used to massacre women and children in remote rural villages and some as young as ten years of age were even used as assassins.

In Spain, the *Euskadi Ta Askatasuna* (ETA - Basque Homeland and Freedom) emerged in 1959 as a student resistance movement opposed to General Franco’s military dictatorship. The group increased its youth members (under the age of 20) from 9 per cent in the 1970s to approximately 60 per cent of the organisation by 2005. Its push to seek out new members from a younger demographic (which was a marked change from the past when the ETA was very selective in its recruitment) has ensured its continuity. In fact, the ETA’s ability to revitalize itself as a whole has been largely due to its own youth organisations, Jarrai (followed by Haika and Segi). The ETA survived until 2018 but had declared a ceasefire in 2010.

In India, Samuel highlighted the case of the Mumbai attacks in November 2008, in which ten coordinated assaults left 165 civilians and security personnel dead. He pointed out that one of the common threads that bound the attackers together was their relatively young age. Besides the eldest terrorist, who was 28 years old, the average age of the remaining nine terrorists was only 23 with the leader, Ismail Khan, being 25 years old.

In the Philippines, the Abu Sayyaf Group (ASG) has been fighting for an independent Islamic state for the country’s Muslim minority. The founder of the ASG, Abdurajak Janjalani, was in his early 20’s when he was radicalized and only 26 when he formed the ASG. His replacement was his younger brother Khadaffy Janjalani, who led ASG when he was only 22. In 2009, the ASG was led by Yasser Igasan who was only 21 years old when he joined the movement. Besides the ASG, the Rajah Solaiman Movement (RSM), which originated from a cell of militant students and teachers at a religious school in Luzon, was founded by Ahmad Santos who had been indoctrinated when he was only 21 years old. The RSM was infamous for its role in carrying out the Superferry 14 bombing on 27 February 2004, which led to the death of 116 people and is to date considered the worst maritime terrorist attack. The alleged perpetrator of the act was Redento Cain Dellosa, who was in his mid-20s.

In Iraq, Al-Qaeda had also featured young people prominently. The group had developed videos targeting youth for recruitment. The videos featured the group discussing their strategy for training children to become suicide bombers and showcased young boys making “statements promoting slaughter and declaring their allegiance to al-Qaeda.” Videos were released containing scenes where “children would interrogate and execute victims, plant improvised explosive devices [IEDs], and conduct sniper attacks against security forces.” Also in Iraq, insurgent groups were alleged to have paid between US $50 and US $100 to teenagers for planting IEDs, and shooting a mortar or firing a machine gun at coalition troops. The number of children involved in terrorism in Iraq was clearly seen when during the first 12
months of the US invasion in Iraq, the US forces had detained more than 100 juveniles, a number which increased to 600 juveniles as of 2008.51

Radicalization in Schools

History has shown us that school children have oftentimes participated in various organizations that promote or carry out acts of violence. Their roles have varied from offering logistical support, serving as “mules” or “lookouts”, to fundraising and actual participation in attacks.

In Indonesia, violent extremists are deliberately targeting and recruiting students from high schools.52 This is not surprising, as 23 per cent of the entire population of Indonesia are in high school, making this a key location for recruitment for violent extremists.

From this author’s research in Southeast Asia, schools have oftentimes been the “go-to” source for terrorists to actively radicalise and recruit.53 For instance, hundreds of Indonesians, Malaysians and Filipinos, many of them students, volunteered as mujahideen warriors to fight in Afghanistan and subsequently returned radicalized.54 B. Singh, a university professor from Singapore, observed a growing trend of students being radicalized in Indonesia.55 In light of this, Indonesia’s Vice-President Ma’ruf Amin was tasked by President Joko Widodo to lead a government campaign to counter this phenomenon. Vice-President Amin highlighted that extremist ideologies had even reached preschool play groups, observing that “the challenge (was) getting bigger because radicalism has a growing influence on society, not just among civil servants but also students. We even received reports that it has already found its way to the PAUD (preschool play groups).”56 Benny Mamoto, a retired Indonesia Police General, confirmed this, saying that, “they [radical groups] entered into all layers of society, including education.”57 Indonesian violent extremists gained access into schools by assigning their members to join student or youth organizations and subsequently acting as mentors to youths and undergraduates with the purpose of recruiting them in the future.58

In the Philippines, this phenomenon of recruiting youth from institutions of learning is not new either and has been going on since the 1980s. According to Umug, a former terrorist in the Philippines, communist-based insurgents exploited clubs in schools to target and radicalize Filipino youth, specifically those around 17 or 18 years of age. This method of exploiting the education system was subsequently adapted and fine-tuned by other Muslim-based extremist groups. The ASG, for example, had a policy of selecting only the “brightest and toughest students who were willing to fight for their religious cause.”59 Other Muslim groups established religious schools and then provided financial scholarships, making it extremely attractive for students to study in such institutions. Reportedly, Mohammed Jamal Khalifa, the brother-in-law of Osama bin Laden, had established a school in the Southern Philippines with the express intention of recruiting young people for jihad. The youths who began studying in these religious schools did so with hopes of receiving an education to become qualified religious teachers, but were, unfortunately, deceived and subsequently indoctrinated.60

In 2007, the challenge of youth involvement in terrorism was highlighted by Jonathan Evans, MI5 director, when he stated that “extremists were methodically and intentionally targeting young people and children in the UK,” and that groups like Al-Qaeda were recruiting children as young as 15 to wage “a deliberate campaign of terror” in the UK. He further warned that extremists and terrorists were “radicalizing, indoctrinating and grooming young, vulnerable people to carry out acts of terrorism” and that urgent action was needed on the part of the authorities “to protect its children from exploitation by violent extremists.”61 In the same vein, in March 2009, the UK Association of Chief Police Officers (ACPO) highlighted that two-hundred schoolchildren in Britain (some as young as 13) had been reported as having been “groomed by radicalizers” and hence had become susceptible to violent extremism.62 In light of this, schools in the UK have been mandated by law (Section 26 of the 2015 Counter-Terrorism and Security Act) and are required to have “due regard to the need to prevent people
from being drawn into terrorism.” This controversial duty is known as the “Prevent Duty.” The responsibilities for schools include training teachers and staff to be able to identify and recognize children who might be vulnerable to radicalization, and promote fundamental British values that would enable the students to challenge the narrative of violent extremists or terrorists. Furthermore, teachers and staff are required to assess the risk of the students being drawn into terrorism, and build resilience in students by providing them safe-spaces to discuss controversial subjects, while educating them on how they could influence and participate in decision-making.

**Radicalization in Universities**

In the case of universities, Samuel in his research on undergraduate radicalization in Southeast Asia highlighted that “terrorists and extremists have been looking at institutions of higher learning and their students as a source of recruitment and support.” In the eyes of terrorist leaders, such undergraduate students are seen “as a strategic target audience and that by recruiting them, the terrorist network would be able to build up a support base amongst a group that might one day become influencers themselves in the wider community and future leaders.”

In a European study, Peter Neumann observes that universities are “places of vulnerability” due to the fact that undergraduates are young, “often away from home for the first time, feeling quite lost and often experiencing a sort of crisis of identity.” According to him, this makes it easy for extremist groups to pick them up and to say to them: “Come along to our meeting, we are like you.”

This was also reiterated by Kumar Ramakrishna (Nanyang University, Singapore) who notes that the majority of undergraduates who are young are “still maturing both emotionally and intellectually” making them “susceptible to idealistic appeals from charismatic ideologues who seem to have clear-cut answers for the confusion that these undergraduates might feel about the world around them.” The reach and significance that violent extremists and terrorists can have in a university can clearly be seen in Afghanistan where groups like the Taliban (meaning “students”) take full advantage of their access to universities to exploit the mobilizing power of student protests to advance their vested interests. They do this by developing a patron-client relationship with undergraduates to provide assistance and financial support to undergraduate associations as well as opportunities after graduation from university. In return, some university undergraduates promise to become mouthpieces of violent extremists for advocating and disseminating their rhetoric, propaganda, and ideology within the university environment.

Universities are at times also used as a propaganda arena by foreign students and lecturers from countries in conflict zones. In such instances, lecture sessions are often “hijacked” to “preach” and explain the injustices and atrocities taking place at home and abroad. Over a certain period of time, such lectures can shape, mould and convince undergraduate students into believing that terrorism as “propaganda of the deed” is the only route available for addressing grievances.

**Radicalization Pathways of Youth**

Better understanding of how and why young people are radicalized and join violent extremist groups is essential in developing strategies on how to prevent and counter their radicalization into violent extremism. Young people join violent extremist and terrorist groups for various reasons. Oftentimes, they have little choice in the matter as they are forced into joining. In Iraq, ISIS kidnapped thousands of children from orphanages, schools, and even their homes, while
also taking over existing schools and teaching their own curriculum. Over one-third of the 6,800 Yazidis that were captured by ISIS in Sinjar in 2014 were made up of children under the age of 14. Another 800 to 900 children were said to have been kidnapped from Mosul for religious and military training. Boko Haram in Nigeria has frequently used mass kidnappings, including the infamous abduction of the 276 Chibok school girls in April 2014 and 110 Dapchi school girls in March 2018. In the case of Somalia, in 1997 alone, Al-Shabaab utilized detention, violence, and intimidation to recruit approximately 1,777 youths.

The UK Government, while acknowledging that there is no single path to radicalization, identified four possible contributing factors that can lead to a young person being radicalized into violent extremism. The factors include:

1. exposure to an ideology that appears to sanction, legitimize, or require violence, often by providing a compelling but fabricated narrative of contemporary politics and recent history;
2. exposure to people or groups who can directly and persuasively articulate that ideology and then relate it to aspects of a person’s own background and life history;
3. a crisis of identity and, often, uncertainty about belonging which might be triggered by a range of further personal issues, including experiences of racism, discrimination, deprivation, and criminality (as victim or perpetrator), family breakdown, or separation; and
4. a range of perceived grievances, some real and some imagined, to which there may seem to be no credible and effective non-violent response.

**Tipping Points to Violent Radicalization**

Research has also shown common indicators for violent extremists which might also apply in the context of young people undergoing religious radicalization. For example, Gartenstein-Ross and Grossman conducted an empirical examination of radicalized individuals in the UK and US to discern the process that lead to them becoming radicalized. They found that firstly, those who were radicalized were familiarized with a very rigid, conservative and legalistic interpretation of religion in which a strong focus was placed on the literal interpretations of holy texts. Secondly, they strictly followed and trust only select religious authorities who were deemed authentic and credible while everybody else was considered a fraud or their teachings were presented as a watered-down and inauthentic version of the true faith. Thirdly, they believed that there were irreconcilable differences which had led to a divide between Islam and the West and that a clash of civilizations was therefore inevitable. Fourthly, there was little acceptance or tolerance with any party that did not fully conform with their theological doctrines and beliefs. Fifthly, violent extremists took it upon themselves to impose their religious doctrines and beliefs on everybody else, and any means towards this end was justified. Finally, there was an element of political radicalization as violent extremist believe that there is a conspiracy by the West against Islam to destroy the religion both “physically and morally.”

**Whole-of-Education Approach: Rethinking Education in PCVE and Terrorism**

There is a growing realization that solely focusing on a military approach or hard power to prevent and counter violent extremism is a strategy that is no longer tenable. Hence, national and international strategies in PCVE and terrorism are focusing more on conditions conducive to the spread of terrorism.

In that regard, education has been described as a “moral enterprise” that has the capacity to develop and shape the hearts and minds of an individual in society. This, in turn, could
potentially be a template for a viable and impactful strategy to address, and possibly reverse, the threat of violent extremism, particularly among the youth. As a result of this, schools and universities have “gained growing importance as platforms for different kinds of prevention protocols or counterterrorism strategies.”

Echoing this, in 2013, former UK Prime Minister Tony Blair highlighted that violent extremism would “never be defeated by security measures [alone]”, adding that “only the education of young people can achieve [its] demise.” Similarly, the United Nations Global Counter-Terrorism Strategy emphasizes the pivotal role of education by reiterating that an effective counterterrorism strategy must take steps to “promote a culture of peace, justice and human development, ethnic, national and religious tolerance and respect for all religions, religious values, beliefs or cultures by establishing and encouraging, as appropriate, education and public awareness programs involving all sectors of society.”

In the same sense, the Ankara Memorandum on Good Practices for a Multi-Sectoral Approach to Countering Violent Extremism was formulated to address the role of government institutions, agencies, and civil society in CVE. The Memorandum reaffirms the role that “educational institutions can serve as an important platform in countering violent extremism,” noting that critical thinking skills, civic education, community engagement, and volunteerism in schools have a potential in turning the tide against violent extremism and terrorism. UN Security Council Resolution 1624 (2005) also stressed the important role of educational institutions in “fostering an environment which is not conducive to incitement of terrorism.” In light of this, considering integrating PCVE into the education curriculum makes eminent sense.

**The Case of “Non-Violent Extremists”**

Being radical in and of itself is not wrong. For example, giving non-whites and women the right to vote and the emancipation of slaves were, in 19th century Europe, considered to be “radical” ideas and seen as going against the status-quo. Thankfully, they were championed by radical political parties, brought to pass, and currently are accepted as the norm in most societies. Radicalism is not the same as extremism although these two concepts are often used interchangeably. The popularity of the concept of radicalization as a term for mobilization to support or engage in acts violence has given radicalism a bad name which is – from the point of view of the history of ideas – partly undeserved. Radical political parties emerged after the French revolution and stood for equality, secularism, republicanism, and democracy. Extremism, on the other hand, emerged in the 20th century and is associated with fascism and communism and other authoritarian and totalitarian movements, including religious movements, some of them violent, others not (or not yet).

Hizb ut-Tahrir (HT, or “Party of Liberation”), for example, targets university undergraduates in certain countries, rejects the idea of the nation-state and the principles of democracy, and instead advocates a return to a caliphate-style theocracy which HT claims to bring about without utilizing violence. However, Ed Husain, a former member of HT, observed that certain world-views even when held without advocating violence, “provides the mood music to which suicide bombers dance.” Echoing this, Abu Bakar Ba’asyir, when asked about his role in motivating terrorists in Indonesia declared, “I am only a craftsman selling knives; I am not responsible for how those knives are used.” He was clear that his role was just to push an extremist idea and how that idea was subsequently interpreted and followed through, was not his responsibility.

Hence, there is a growing concern that extremist groups are developing and disseminating dangerous ideas such as the supremacy of a certain race or religion, the notion that their identity is being “attacked” by the “other,” or even that principles of democracy and election are against God’s will. It is significant to note that developing, holding, and disseminating such ideas is,
in most jurisdictions, not a crime and some would even say, play the role of a “safety-valve,” that allows the youth to express themselves without necessarily resorting to actual violence. On the other hand, there are also those who argue that such ideas act as a possible “conveyor-belt” into violent radicalization. While the final outcome of some of these “non-violent extremist ideas” that are being developed, marketed, and disseminated by extremists to the youth is uncertain - what should our response be? Who would be in the best position to facilitate and develop a comprehensive counter response to that being pushed by the extremist? It is argued here that educational institutions can be equipped to lead this charge in the “marketplace of ideas” for the hearts and minds of our youth.

The Argument for Education as the Primary Line of Defence in PCVE among the Youth

When formulating strategies in countering terrorism, agencies such as law enforcement authorities play an active and often leading role. There is a growing realization that a soft power approach, and in particular, the use of education, is a promising way to move forward in PCVE. That being the case, national governments and the international community must not just pay lip-service but ensure that when they pledge for education to be given a greater role in PCVE, they also ought to implement policies to that end. However, before education can play a more prominent and pivotal role in PCVE, there needs to be the realization among policy makers that violent extremists and terrorists are indeed targeting and recruiting young people. Secondly, it must be recognized that students in educational institutions are vulnerable to such efforts being undertaken by extremists. Thirdly, while being susceptible to the radicalization process, institutions of learning, with proper planning and support, can be “hardwired” to develop in their students a mental and emotional “firewall,” capable of withstanding indoctrination (should it occur) carried out by violent and non-violent extremists. For this potential to be realized, there needs to be a rethinking in the way that PCVE is viewed in the education sector.

Education can no longer be seen as a secondary line of defence; rather, it must be viewed as the primary line of defence against violent extremism and terrorism, for no terrorist attack can take place until and unless potential terrorists are identified, indoctrinated, and recruited. Neumann’s definition of radicalization - “what goes on before the bomb goes off” - indicates that before the physical battle even begins, radicalization must occur and it is precisely this radicalization process that education should seek to engage with and defeat.

Recognizing the primary role of education in PCVE among the youth should lead to a change of mindset in government as well as within the education sector itself. Within the government, education’s elevated standing as a primary player in PCVE, on par with the police and the courts, must be reflected in a National Action Plan (NAP) in PCVE. The role, mandate, scope, and responsibilities of the education sector must be taken into consideration. The Ministry of Education has to ensure that young people studying in institutions of learning are taught values at the primary, secondary, and tertiary levels. Only in this way can a “firewall” against possible future radicalization be installed. This means that the education sector should envision and plan to protect student populations against radicalization to violence in the ten or more years that the student is in an institution of learning. Students ought to be given all that is necessary to be able to withstand the process of radicalization.

Given this challenging role, the education sector needs to evaluate what it has and what it may need, to be in the best possible position to shoulder this responsibility. The educational institutes will need to:

1. Identify specific areas (i.e., cognitive and emotional spheres) where they intend to build resilience and fortitude.
2. Target and teach specific qualities in relation to age levels (for example, focusing on developing qualities such as tolerance and compassion during the primary schooling while emphasizing empathy, appreciation of diversity and critical thinking during the secondary/tertiary schooling, etc.).

3. Seek outside assistance in reinforcing PCVE content to students (for example, by utilizing rehabilitated terrorists, former victims of terrorism, moderate religious and spiritual mentors, social media influencers, and celebrities to heighten the reach, appeal, and impact of PCVE narratives).

4. Develop a syllabus on PCVE that covers all the relevant issues specific to a country and ensure its continuity for the student from primary to tertiary levels.

5. Train specialized teachers at the primary, secondary, and tertiary levels not only to mentor and guide the students in discussing PCVE issues, but also in being able to recognize and detect possible signs of radicalization.

6. Develop and build networks of specialised expertise, for example psychologists, youth counsellors, religious leaders, and even the police, for teachers to seek help or even to refer students who are showing signs of worrying behaviour which might be beyond their ability to handle.

7. Develop a monitoring and evaluation mechanism to assess, rectify, and modify all the efforts being undertaken at the working and policy levels within the education sector.

The potential of the education sector in facilitating and developing policies and interventions in the field of PCVE for the nation has yet to be fully explored. Given education’s reach and daily access (via nursery, primary, secondary, vocational/tertiary schooling) into the lives of a huge percentage of the population (i.e., from the ages six to seventeen and even beyond) for a reasonably lengthy period, particularly during the formative and vital years of an individual, it would be a tremendous waste, if more is not expected and indeed done by national education agencies when it comes to PCVE.

Essentially, a holistic and comprehensive approach is needed when looking at education and PCVE. A whole-of-education PCVE approach should seek to impart and instil values and knowledge associated with PCVE in a comprehensive and methodical manner, through various approaches and interventions, spanning the students’ entire academic and extra-curricular journey, from nursery to university.

**Integrating PCVE in the School/University Curriculum**

As said before, the goal of the education sector should be two-fold. Firstly, to protect a student from violent extremism while in an institution of learning and secondly, to impart and equip students with all that is necessary to prevent them from ever considering violent extremism in the future. Given this lofty ambition, it is essential that the PCVE component be integrated into the entire curriculum; it should also include vocational and religious elements of the student while in school and possibly into higher learning institutions such as the universities. PCVE should essentially be “aimed to be carried out principally as a part of everyday schoolwork.”

It is important to note that for a PCVE mindset to be successfully imparted on a student, it is not just knowledge that has to be transferred but also values. Both “knowledge” and “values,” if properly constructed and delivered, have within them powerful defensive and even offensive characteristics that can protect an individual against succumbing to extremism. However, these components of “knowledge” and “values,” if merely shoved onto the student, would look like propaganda or preaching and would greatly diminish their effectiveness. Hence, what is needed is a “vehicle” to carry both these components of knowledge and values into the hearts and minds of the student. The possible “vehicles” that could be utilized to carry these two components would include:
1. academic subjects like history, ethics/moral education, philosophy, and religious studies;
2. study of biographies of noted individuals as well as organizations;
3. sports;
4. extra-curricular activities within uniformed bodies, clubs and societies;
5. volunteerism;
6. student exchange programs; and
7. promoting better understanding and appreciation of differing cultures, practices and religions.

These approaches will be discussed below.

**PCVE “Vehicles” in Schools**

There are seven PCVE ‘vehicles’ that will now be discussed.

**Academic Subjects**

Academic subjects in schools and universities like history, ethics/moral education, philosophy, and religious studies can integrate PCVE components in their content. These subjects already touch upon issues such as violence, conflict resolution, the history of individuals/groups manipulating religion, etc. With proper planning and training, these academic subjects can be utilized to create knowledge and impart values on the sacredness of life and the total disregard that terrorists have for people’s lives.

**Imparting PCVE Elements in Biographies of Noted Individuals and Organizations**

Young people are oftentimes less interested in theories, concepts, and models and more interested in real-life individuals. Violent extremists are fully aware of this and oftentimes exploit this by painting their leaders and fighters as courageous heroes and martyrs, fighting for a noble cause. In this regard, PCVE initiatives need to showcase positive role models that young people can adopt as their heroes. Individuals such as Mahatma Gandhi, Martin Luther King Jr., Nelson Mandela and Florence Nightingale as well as organizations such as Doctors Without Borders (Médecins Sans Frontières) and the Red Cross/Red Crescent Movement can provide inspiring and positive examples for students to get to know and emulate. Efforts could also be undertaken to identify and highlight young and current “heroes” that might be more relatable to the current generation. The inspiring stories of role models such as Malala Yousafzai, Greta Thunberg, Ishmael Beah, and Nadia Murad can be used in short documentaries, YouTube video clips or comic books to reach and impact youth in both schools and universities – showing how everyone can make a significant difference in the world.

**Sports**

Sports have the capacity to play a pivotal role in “fostering communications and building bridges between communities in conflict.” In January 2014, the European Commission, in its recommendations to the European Parliament suggested that “sports be included in broader education efforts to build resilience against violent extremism.” Specifically on PCVE, a study conducted in 2018 noted that sports-based programmes had the capacity to build in vulnerable youth core life-skills which, in turn, are essential building blocks when it comes to
preventing violent extremism.\textsuperscript{95} In this regard, educational institutions have yet to fully exploit the positive role that many (but not all) sports can play in PCVE.

Extra-Curricular Activities within Uniformed Bodies, Clubs and Societies

Organizations, societies, and clubs in schools and universities such as the Boy Scouts,\textsuperscript{96} Girl Guides,\textsuperscript{97} the Interact Club,\textsuperscript{98} the Leo Club,\textsuperscript{99} or Toastmasters\textsuperscript{100} are already involved in trying to encourage their members to become “agents of positive change who inspire others to action.”\textsuperscript{101} Through such bodies, members are trained “in life skills, leadership and citizenship”\textsuperscript{102} as well as skills to communicate and positively impact the lives of others. These organizations also actively encourage and promote social diversity and mixing in terms of race, culture and religion. Hence, recognizing the need for a sense of identity, adventure, self-worth, significance, and security among young people; the programs and activities organized by these uniformed bodies, organizations or societies could be “leveraged” upon “to deter youth from embracing extremist ideologies.”\textsuperscript{103}

Volunteerism

Volunteerism is a powerful way for students to engage in something meaningful while also giving them a sense of significance.\textsuperscript{104} Kruglanski and his colleagues did extensive research on how the quest for personal significance is a major motivational factor that has pushed some individuals towards violent extremism.\textsuperscript{105} In this regard, volunteerism has the potential to allow students to contribute in a meaningful way to a cause that would give them a sense of purpose. This would then, to a certain extent, mute the appeal and call of violent extremism to the youth for them to do something of significance.\textsuperscript{106} Realizing this, in 2012, the Ministry of Higher Education in Malaysia launched the Yayasan Sukarelawan Siswa (YSS) or Student Volunteers Foundation. The focus of this foundation is to “promote, educate and guide students to volunteer to promote world peace and foster a spirit of camaraderie by engaging in community services at home and abroad.”\textsuperscript{107} The idea to channel youthful enthusiasm and energy into altruistic rather than destructive directions is open to greater development.

Student Exchange Programs

Student exchange programs at schools and universities allow young people to travel, both within and beyond their country’s borders and experience for themselves foreign and different cultures. This, in turn, has the potential to dispel ignorance and prejudice as well as sow seeds of appreciation for other races, religions, and cultures. Based on contact theory, the assumption is that “meeting and interacting with others who are different will challenge stereotypes and biases” and can make young people more resilient to withstand recruitment by extremists.\textsuperscript{108} According to a Malaysian student who participated in a student exchange program with Japan, staying in the homes of foreign students allowed him to “learn new cultures, form new friendships and encourage people to be open to new things.”\textsuperscript{109}

It is also important to point out that student exchange programs need not only be confined to travel outside one’s own nation. Countries that have multiple races, religions, and cultures can utilize such exchange programs to enable their students to have a short experience outside their own racial, religious, and cultural confines. In addition, travelling and experiencing other cultures does not only benefit the student-traveller but also allow the host family/school/university to “take a peek” into a foreign culture. This has the potential to provide practical opportunities to realize that we are all “connected” and can become “global
citizens,” and that the “other,” so often demonized by populists and extremists, is not so different.\textsuperscript{110}

**Promoting Religious and Cultural Literacy Among Students**

Ignorance and prejudice are powerful tools in the hands of violent extremists and terrorists. Misinformation and disinformation coupled with selective interpretations of religious texts and highlighting only certain negative news about another race, creed, or ethnicity has the potential to paint the “other” as the “enemy” responsible for everything conceivably wrong with one’s own “tribe.” The only way to counter systematic brainwashing by extremists is to actively create awareness of the “other” as well as building bridges to them. In this regard, education via religious literacy\textsuperscript{111} is critical in promoting knowledge of others and in dispelling ignorance. According to Diana Moore, religious literacy can be defined as the ability to discern through multiple lenses and analyze the convergence of religious, social, political, and cultural spheres that have occurred throughout history.\textsuperscript{112} The consequences of religious illiteracy, according to Moore, include fuelling culture wars, curtailing historical understanding, and promoting religious and racial bigotry. These are the very triggers and drivers that have the potential to lead young people into the hands of extremists, who then skilfully manipulate and exploit grievances.\textsuperscript{113}

Besides educating students in schools and universities on the characteristics and contributions of people from other cultures, there should also be efforts to ensure that this education continues beyond the classroom. Field trips to the places of worship of other religions, community service in areas where the residents are of different ethnicities and cultures to that of the student, and visiting homes of people from other backgrounds could be systematically planned and implemented at various stages of students’ educational journey, taking into account sensitivities involved. In the case of Malaysia, a national PCVE undergraduate program was carried out in January 2020 by the International Islamic University with support from the Ministry of Youth and Sports. The organizers conducted visits to various places of worship as part of the program. While there were “initial reservations,” briefing sessions followed by open and frank discussions before the visits were vital in getting the necessary buy-in from the participants and other parties involved. The feedback received from the participants was “positive” and the participating students felt that the visits “promoted understanding, tolerance and respect.”\textsuperscript{114}

**The Role of the Teacher**

Paulo Freire, in his book *Pedagogy of the Oppressed*, introduces the term “banking model of education” which he describes as a form of education that is fundamentally one way only. In his model, instead of communicating, the teachers’ function is simply to issue directives and provide information for the student. Under this “banking” concept of education, the students’ responsibility was solely to receive, file, and store the “deposits.”\textsuperscript{115}

At present, however, the idea of education has evolved from a process of transferring knowledge from the teacher to the student to a more student-centered approach, wherein the student is more involved in the process of acquiring knowledge, skills, beliefs, values, and the culture of the society that he or she is placed in.\textsuperscript{116}

Specifically, when it comes to teaching elements of PCVE, it must be stressed that the transfer of knowledge is not the primary goal. *Knowledge* on counterterrorism, terrorism and extremism in general, and the violent radicalization process in particular, will be of little use in preventing a student from being indoctrinated and subsequently recruited. What is desired instead are the *values* transmitted to the student which are then internalized (i.e. accepted and
believed) by the student and subsequently practised and manifesting itself in the behaviour of the student. For this process to take place, the role of the teacher is pivotal. Given this, when we look at turning the institution of learning as a channel to counter extremism, the teacher will be the focal point of this initiative, as they are in the “unique position to affect change, impart affirmative messaging, or facilitate intervention activities due to their daily interactions with students.” However, given the range of responsibilities and the complexities involved, careful consideration should be undertaken when identifying and selecting the teachers intended to carry out these tasks. Rather than training all teachers to undertake this responsibility, it would be worth considering selecting a handful of teachers in each institution of learning to be the focal point of this initiative. Teachers involved in counselling, psychology, or student affairs, given their closer dealings with students, could be potential candidates.

However, given the magnitude of the problem of possible radicalization among the youth, there is also the possibility of considering all potential teachers undertaking their training, to be at the very least, exposed to the basics of PCVE and terrorism. The European Radicalisation Awareness Network (RAN) noted that “schools should invest in basic training for all teaching staff (not only those teaching politics, history or ethics) so that they are equipped to detect the signs of radicalization and intervene effectively.” This could be done by ensuring that all participants in teacher training colleges are taught and are aware of the main issues pertaining to the radicalization process targeting young people. In this regard, while all teachers might not be given the responsibility of conducting PCVE initiatives in institutions of learning, all teachers would nevertheless still be aware of the fundamental issues involved and would be able to detect possible signs of radicalization which they can subsequently discuss with the trained specialized teachers.

The training for specialist teachers would essentially be focused on equipping them with the skills to shift from just providing knowledge and information on a particular subject to that of being a guide or mentor facilitating the discussion on the subject of PCVE. Specifically, these teachers/mentors/guides would play a vital role and therefore need to be trained in:

1. setting the scene and preparing a “safe space” to discuss the subject;
2. building trust to allow the students to openly share their views, fears, and concerns;
3. maintaining their own credibility to ensure the best chance for the students to consider and adopt the material being presented;
4. displaying calmness and composure when confronted with difficult issues and questions;
5. exhibiting humility to avoid students from feeling patronized and belittled in any way; and
6. demonstrating gentleness, creativity, and even a sense of humour to maximize the impact of the content imparted to the students.

Firstly, the teachers would “set the scene” when it comes to introducing the subject to the students. They would play a crucial role in assessing the environment, background, and impact of violent extremism and terrorism on the students before even presenting the content. In this regard, teachers would be trained to contextualize the issues based on the particular time, and setting in which the students find themselves.

Secondly, the teacher would need to earn the trust of the students for them to feel safe to voice their fears, doubts, and concerns with regards to the issue. It must be stressed that winning the confidence and trust of the student is not immediate nor automatic, but there are steps that could be taught to teachers, that could, in time, lead to the students bridging the “trust deficit” that might possibly exist.

Thirdly, given the sensitivity of the subject material, teachers must maintain their credibility at all times. Hence, it is of paramount importance that their intentions, words, and behaviour, not only when teaching the subject per se, but as a whole, does not exhibit any signs
of racism, bigotry, or prejudice. In the event that they do, any hope of building a mental and emotional “firewall” through the material presented, would be lost and could even aggravate the situation, leading to further polarization.

Fourthly, given the controversies surrounding this issue, teachers should be prepared and trained to face difficult and perhaps even hostile questions, comments, and opinions with calmness and composure. It is in this sometimes “hostile” environment that teachers can and should take the opportunity to impart the valuable example of dealing with opposing views held by “difficult” individuals. Calmness and composure will not only be essential when dealing with controversial and emotionally-charged issues, but could possibly form the basis which students can use as an example when they in-turn have to deal with “difficult” people themselves.

Fifthly, teachers should display humility when presenting PCVE content, to ensure that the students do not end up feeling patronized or belittled. Oftentimes, the manner in which PCVE content is presented to students is typically one of a “master-disciple” dynamic. Based on the premise of “describing the problem” and subsequently “providing the solution,” the content presented is a “close-system” in which there is little need for input from the students simply because everything has already been “thought of,” “figured out” and “resolved” and all that the student is required to do is to “follow the set of instructions given.” This condescending approach does not allow the student to contribute in any meaningful manner. Humility, on the other hand, will allow the teachers to acknowledge that there could be possible weaknesses in the system that has led to violent extremism and that input and effort from all, particularly the students, is essential in resolving this issue and making things better. This admission, followed by the act of “seeking help” from the students to resolve the problem, could prove pivotal, as students realize that they can now participate and have a meaningful role in actually addressing and resolving grievances. Not only could this help in encouraging participation from the students but it could also play a role in muting the appeal of the violent extremist for young people to join them.

Finally, teachers would be trained to maximise the impact of the PCVE content by displaying gentleness, creativity, and even a sense of humour. Gentleness would be essential in conflict or difficult situations where hurt, resentment, and bitterness are present among the students. “Creative foresight” in bringing up the subject, making it relevant, and even slipping through the mental and psychological defences of the students would go far in ensuring that the content is well-received and impactful. Using humour has the potential of defusing an emotionally-charged subject, enabling the teacher to convey a point in a non-confrontational manner.

The Need for External Support

While teachers play an important role in PCVE in educational institutes, it would be detrimental to assume that they are the only channels that one could use to reach the students. Role models and influencers can be found in different walks of life. In this regard, former rehabilitated terrorists, victims of terrorism, and influencers/celebrities/youth heroes have tremendous potential to make a significant impact when it comes to PCVE among the youth.

Rehabilitated Terrorists

Rehabilitated terrorists have a story that people in general, and youths in particular, would want to listen to. Their background, choices that they have made, and experiences that they have undergone, not only make them intriguing speakers but also gives them the “street cred” that teachers or lecturers might not necessarily possess in the eyes of the students. For example,
Nasir Abas, a former senior leader of Jemaah Islamiyah in Indonesia, has oftentimes been invited to reach out to students both in high schools and universities across Indonesia. In Malaysia, the Southeast Asia Regional Centre for Counter-Terrorism has used rehabilitated former terrorists (who were themselves young) to reach out to university students; the impact caused was significant.

However, in most cases, utilizing such individuals has been on an ad-hoc basis, limited by issues of logistics such as travel. This however, could be easily resolved by using video testimonies of selected rehabilitated terrorists and screening them to students in schools and universities in a structured manner. The author of this chapter utilized this method by screening a video clip of Arno Michaelis story, a founding member of one of the largest skinhead organisations in the world in schools and universities all over Malaysia. What was intriguing was that while the skinhead organization and the ideology of white supremacy had very little traction in Malaysia, many Malaysian students and undergraduates were nevertheless visibly moved by Arno Michaelis’s narrative, making it a valuable tool in reaching out to students.

Victims of Terrorism

Victims of terrorism have a unique voice and provide a “powerful emotional narrative” that has the potential to “reinforce dissatisfaction” among young people over the method and the approach taken by terrorist groups. Max Boon, a victim of the 2009 Marriott Hotel bombing in Jakarta who lost both legs, has used his experience to reach out to high-school students in Indonesia. What is unique is that he has partnered with rehabilitated terrorists in reaching out to Indonesian youth and this approach has inspired many. In this regard, it is unfortunate that while many young people are very familiar with the rhetoric and propaganda of terrorists, they have heard very little from the very people who have suffered the most from terrorist attacks. In this regard, the narrative of a victim is a powerful tool that has the capacity and the capability to counter the often times evocative premise that the terrorists are representing and fighting for a victimised group of people. For example, mothers who have suffered at the hands of violent extremists and terrorists have an extremely powerful message that would certainly resonate, and not just with youth. Mothers who have lost their children and collective groups of women such as Mothers for Life and Women without Borders can work with educational institutions to vividly showcase the dangers of violent extremism. The poignant letter that the group Mothers for Life wrote to Abu Bakr al-Baghdadi on Mother’s Day, grieving for their children who died as a result of terrorism, is a powerful example that should be read in all institutions of learning. Hence, as highlighted by Schmid, “victim and survivor voices need not only be heard, but ought to be amplified.” In this regard, educational institutions could play a significant role in being the conduit to channel the stories of such victims and allow the students to see past the propaganda of violent extremists.

Role Models and Influencers

While it is essential to ensure that qualified and trained people like teachers and lecturers are used to present content on PCVE to students in educational institutes, it is also imperative that such initiatives utilize other people; role models whom the youth look up to. Far too often, there is a disconnect between experts speaking to the young people and young people listening to what is being said. To a great extent, the receptivity issue on the part of young people would be better tackled should they be addressed by the right people; the “right” people being defined as the people that the students look up to and might aspire to become. After identifying such individuals, the onus would then be on the authorities to seek them out and get their assistance
to become “messengers” on the issue of PCVE. Among the possible people that the youth look up to include actors, singers, sports personalities, and social media influencers. Getting celebrities to speak on issues of national and international interests is not new, as seen in the case of the United Nations High Commissioner for Refugees (UNHCR) appointing Angelina Jolie as a Special Envoy in April 2012. Not only do these celebrities have a large following and reach (on-line as well as off-line) but they also have the charisma and “pull” to get messages across to the young people. While not all celebrities would be suitable and there would be some who are suitable but might not be interested, there would certainly be those who are both well suited to speak on PCVE issues to the youth and willing to take upon that role. In Malaysia, PCVE programmes targeting university undergraduates have experimented with using local celebrities including singers, YouTube influencers, beauty queens, sports personalities, and television actors to both attract young people and present them positive messages linked to PCVE – with considerable success.

**The Need for Education to ‘Reclaim’ Social Media**

A 2013 RAND study highlighted that the Internet has increased the opportunities for an individual to become radicalized and can also act as an “echo chamber” in many cases. Education must play a role in reclaiming social media from extremists, not just by learning and understanding the basics of electronic intelligence and cyber security but also by fully exploiting the internet’s potential in PCVE.

A possible reason the internet has oftentimes been cited in playing a role in the radicalization process could simply be due to the “content-imbalance” in favour of the violent extremist or terrorist narrative when compared to more moderate and balanced views. Simply put, on certain issues, violent extremists and terrorists, together with their sympathizers and supporters, appear to offer far more “attractive” content, both in terms of quantity and quality, targeting young people on the internet. Given this scenario, efforts have been undertaken by various specialized organizations to correct this “imbalance” by putting out counter- and alternative narratives to that of violent extremists. The Sawab Centre in the United Arab Emirates (UAE) and the Global Engagement Centre (GEC) in the US are two good examples. However, their actual – as opposed to intended – audience might not necessarily be vulnerable young people and their ability to reach out to youths from different cultures and geographical locations might prove to be challenging given their affiliations and backgrounds. In this regard, the education sector would be remiss if it opts to solely rely on specialized strategic communications organizations to play the role of countering and debunking the narratives of violent extremists.

In such circumstances, the education sector could take a leading role in conceptualising strategies to ensure that students are better equipped when being targeted by extremists over the internet. The first step for the education sector would be to ensure that all PCVE-related content be digitalized and repackaged into attractive formats (digital comics, video animation, on-line games, and quizzes) – formats that appeal to the young generation. This would encourage students to reach out to other sources than those disseminated by terrorist groups and their supporters. This could possibly contribute to correcting the content-imbalance we see at present.

Secondly, institutions of learning, particularly universities, could start initiating programs in which countering the narratives of violent extremists are taught to undergraduates. This, in turn, would be followed by the undergraduates themselves starting to develop and disseminate their own narratives. In this regard, the author was involved in organizing the Students Leaders Against Youth Extremism and Radicalization (SLAYER) workshops which brought 100 university undergraduate leaders from various races, religions and cultures from all over Malaysia together over a period of two-and-a-half days in April 2017. The participants were
trained in the workshops to conceptualize, develop, and disseminate digital PCVE products. With their assistance, the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCCT), doubled and later tripled its capacity to produce PCVE-based digital content.\textsuperscript{142}

It is also significant to note that PCVE narratives and messaging coming from the young people themselves carry more credibility in convincing their fellow peers when compared to messages solely developed by educational authorities. An emphasis on getting the youth to both create and disseminate counter- and alternative narratives should be part of a larger effort to train students to be positive social media influencers\textsuperscript{143} and “digital story-tellers” and reach out to their fellow digital peers.

Finally, education will only “reclaim” social media if the authorities are willing to seek genuine cooperation and collaboration with young people. Numerous digital PCVE initiatives targeting the youth are facilitated by bureaucrats who are out of touch with the intended target audience, do not understand the messaging habits of young people, are not recognised by the young people as being credible messengers and do not even themselves use the digital media utilized by the youth. For educational institutions to make an impact via social media, the students should not be seen as mere “clients” but rather as “partners”; with both sides having the common objective of preventing and countering violent extremism.

\textit{Inculcation of ‘Mental and Emotional Firewalls’ in Students}

The education sector could conceptualise, develop, and impart both mental and emotional “firewalls” into the hearts and minds of the students. In this regard, certain values, skill-sets and awareness such as critical thinking, empathy; diversity; resilience; and awareness on the failures of violent campaigns and the power of nonviolent social movements should be developed and institutionalized into the education system. These firewalls could provide a barrier against the radicalization process targeting the students.

\textit{Firewall 1: Critical Thinking}

Institutions of learning such as schools and universities should play an essential role in developing and facilitating critical thinking among their students to enable them to make sound choices and decisions when confronted with the ideology, rhetoric, and propaganda of violent extremists.\textsuperscript{144} All students should be taught basic cognitive skills such as how to distinguish facts from opinions, identify unstated assumptions and biases in an argument, evaluate the reliability of evidence presented to them, etc.\textsuperscript{145} Critical thinking can be integrated in almost every subject, e.g. civic education, religious studies, languages, science, and philosophy. This is essential as skills like critical thinking allow the youth to see multiple perspectives before coming to a well-reflected perspective of their own.\textsuperscript{146}

\textit{Firewall 2: Empathy}

Empathy has been defined as the capacity to understand and feel what another person is experiencing; it also includes the capacity to place oneself in another person’s position and act altruistically towards persons in need. Experts are of the opinion that if empathy and compassion are nurtured, extremism could be reduced and with that, the propensity for violence diminish.\textsuperscript{147} However, it is also significant to note that empathy needs to be taught in a nuanced and balanced manner. If empathy is only extended to one’s own group (whether racial, religious, or political), it can actually make an individual justify acts of violence to the “other” group.\textsuperscript{148} Hence, when PCVE programmes focus solely on enhancing empathy for one’s own
group, there is a potential for conflict escalation. However, if the PCVE intervention develops a balance between the empathy felt for members of one’s own group and empathy felt towards the suffering of outsiders, individuals are less likely to inflict violence on the “other.” Hence, the education system needs to conceptualize and implement a curriculum and syllabus that can instil a sense of empathy and solidarity not only with members of one’s own group, but also extends emotional bonds to members of the “other” groups at home and abroad.

**Firewall 3: Diversity**

Diversity can be defined as a range or variety of different things. In the context of human behaviour, it would include an understanding that every individual is unique and recognizing and appreciating individual and group differences. The United Nations Development Programme (UNDP) considers the rejection of diversity in society as one of the drivers of violent extremism. Hence, in multi-racial, multi-religious, and multi-ethnic societies, accepting diversity is paradoxically the key to achieving greater unity, which is a formidable “hedge” against violent extremism. In this regard, diversity-education plays an essential role in ensuring that differences, so long as they are within the ambit of the law, are indeed an asset and something to be respected and appreciated. Students in schools and universities should be taught to learn to respect the diversities of cultures, races, religions, opinions, thoughts and practices. They need to understand that diversity has the potential to make a society or a nation richer and even stronger. Wherever there is diversity, there is also a need for respect and tolerance for opinions and practices which differ from one’s own. On the practical side, students should be taught on how to express their ideas and, equally important, accept differing ideas with respect and tolerance. Students need to learn to “disagree without being disagreeable.” That should be translated into their thinking, conversation, and behaviour; both off-line and on-line. In this regard, the educational authorities need to creatively and boldly conceptualize policies and implement interventions that will be able to carry this powerful truth.

**Firewall 4: Resilience**

Resilience has been defined as the ability to mentally or emotionally cope with a crisis and/or to return to a balanced pre-crisis status quickly. Simply put, it is the ability to recover from adversity. Oftentimes, students are made vulnerable due to the adverse circumstances to changes in their environment and these can act as tipping points to make them ready for radicalization.

The reality is that there will be times in the lives of a student where he or she might undergo a crisis or face a problem. Education policy makers in Malaysia, for example, have noted that resilience is a quality that is generally lacking among many Malaysian students. This might also be the case in other countries. The Australian Strategic Policy Institute (ASPI) noted that students in schools need to build resilience as they are in the “frontline of countering violent extremism.” Hence, there might be a need to strengthen resilience among students by teaching them how to cope with existential as well as less serious problems. Hence, resilience training has the potential of equipping such students with tools necessary to bounce back from a crisis, thereby eliminating the temptation to seek council, friendship, or solutions for their problems from extremist recruiters.
Firewall 5: Awareness on the Failure of Violence and the Power of Nonviolence

Extremists oftentimes greatly exaggerate their case that violence can bring about the change that they so desire and that there are no other options than rebellion in the form of terrorism. However, terrorist groups rarely reach their goals. To understand the efficacy of both non-violent and violent approaches to conflict, Chenoweth and Stephan developed the Nonviolent Campaign and Outcomes (NAVCO) data sets in which they analysed 323 violent and non-violent resistance campaigns. According to them, “the most striking finding is that between 1900 and 2006, non-violent resistance campaigns were nearly twice as likely to achieve full or partial success as their violent counterparts.”

In reality, civilian populations have oftentimes organised themselves successfully, utilizing various non-violent resistance methods such as boycotts, strikes, protests, and organized non-cooperation to exact political concessions and challenge entrenched power. For example, non-violent methods were successfully used to remove autocratic regimes from power in Serbia in 2000, in Madagascar in 2002, in Georgia in 2003, and in Ukraine in 2004-2005. Non-violent action was also instrumental in forcing the Nepalese monarch to make fundamental constitutional concessions in 2006. Hence, there is an urgent need to revisit the premise that non-violent action is weak and armed struggle is strong when it comes to address grievances and prevail in conflicts.

Not only is there a need to further develop strategies of nonviolent action, it is also imperative that educational institutions play a pivotal role in ensuring that such ideas and models are publicized, taught and disseminated to students. This is because at present, the narrative of the terrorist that “violence is the only way” is so prevalent that oftentimes, it is seen as the immediate default setting when dissatisfied people are faced with injustices and repression. Given this, students need to be taught that peaceful conflict resolution and non-violent forms of struggle are not only available but that these are also often more effective than the use of arms. In this regard, it is important to note that Samuel’s quantitative study of approximately 8,900 undergraduates in Indonesia, Malaysia, Singapore, the Philippines, and Thailand revealed that the majority of the students believed that the more people know about alternatives to terrorism for waging conflict, the greater receptivity for such options as viable models to address grievances and resolve conflict.

Conclusion

The reality on the ground suggests that violent extremists often look at educational institutions as a potential threat to their existence. Hence, the increase of lethal attacks upon schools and universities in many parts of the world. Somewhat paradoxically, terrorist leaders also look at educational institutions in terms of their recruiting potential for both foot soldiers and future leaders of their organizations.

Authorities have, in many cases, been slow in protecting the infrastructure of educational institutions from physical attacks and even slower to protect the hearts and minds of the students from radicalization efforts by violent and non-violent extremists. More often than not, PCVE has been given a narrow role in educational programs, oftentimes limited to a single stand-alone module presented to the students. However, education has a tremendous potential of playing a far bigger and pivotal role in PCVE amongst young people, given the lengthy duration that most children spend in educational institutions. Most governments have yet to realize this opportunity to prevent radicalization.

There is therefore an urgent need to revisit the role of education in PCVE in institutions of learning and, wherever possible, expand and strengthen the education sectors’ mandate, resources, and delivery mechanisms to become a primary source for PCVE among the youth.
Thomas Koruth Samuel is a consultant with the United Nations Office on Drugs and Crime (UNODC) and the United Nations Development Programme (UNDP). His main areas of interest include Preventing and Countering Violent Extremism (PCVE), countering terrorist narratives, the role of education in Countering Violent Extremism (CVE) and youth radicalization. He started off as a volunteer Health Officer for World Vision East Timor in 2003. Thomas Samuel has an Honours degree in Biomedical Technology, a Master’s degree in Strategic and Defence Studies and is at present pursuing his Ph.D., focusing on the role of the quest for personal significance in motivating terrorism among Malaysian youths. He has been a Senior Fellow with the International Centre of Excellence for Countering Violent Extremism (Hedayah Centre) since 2014. In 2018, he was appointed as a member of the Commonwealth CVE Cadre of Experts.
Endnotes


8 Ibid.


29 Busari 2018.
33 The Express Tribune, 2016.
34 Veenkamp, Ivo and Sara Zeiger, ‘Countering Violent Extremism: Program and Policy Approaches Relating to Youth through Education, Families and Communities’; in: Lombardi,
Marco et al. (eds.), *Countering Radicalisation and Violent Extremism Among Youth to Prevent Terrorism*. Amsterdam: IOS Press, 2015, pp. 151-161.


36 Samuel, T.K., *Undergraduate Radicalisation in Selected Countries in Southeast Asia*. Kuala Lumpur: Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), Ministry of Foreign Affairs, Malaysia, 2018b, p. 34.


39 Ibid.


45 Samuel, T.K., *Reaching the Youth: Countering the Terrorist Narrative*. Kuala Lumpur: Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), Ministry of Foreign Affairs, Malaysia, 2012, p. 6


47 Banlaoi, Rommel C., *Youth as Victims and Perpetrators of Terrorism: The Philippine Case*. Paper delivered at the International Conference on Youth and Terrorism organised by the Ministry of Information in collaboration with the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), Kuala Lumpur, Malaysia on 26 February 2009.

48 Ibid.


51 Curcio, Sharon, ‘The Dark Side Of Jihad: How Young Men Detained At Guantanamo Assess Their Experiences’; in: Benard, Cheryl, (ed.), *A Future for the Young: Options for Helping Middle Eastern Youth Escape the Trap of Radicalization*. RAND’s Initiative on

Samuel 2012.

Ibid., pp. 16-17.

Welch 2015, pp. 7-8.

Professor Bilveer Singh, National University of Singapore, personal communication, 14 April 2020.


Ibid.

Samuel 2012, pp. 15-16.

Ibid., p. 17.

Ibid., p. 16.


Ibid.


Associate Professor Kumar Ramakrishna, Nanyang Technological University, personal communication, 23 January 2018.


Professor Bilveer Singh, National University of Singapore, personal communication, 4 March 2018.

Lecture by Associate Professor Kumar Ramakrishna titled ‘Radicalisation over the Internet: Radicalism, Extremism and the Transition to Real-Life Violence’ for the ‘Social Media in a Crisis – Effective Engagement in the Digital Age Workshop’ organised by the Centre for Excellence in National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore in October 2012.

91 Niemi et al. 2018.


94 As cited in Fink et al. 2015.


100 Toastmasters, Available at: https://www.toastmasters.org/ accessed on 22 April 2020.

101 Scouts, ‘What we do.’


104 Samuel 2018, p. 125.


106 Veenkamp and Zeiger 2015.

107 Yayasan Sukarelawan (YSS)/Student Volunteers Foundation. Available at: https://sukarelawansiswa.my/ accessed on 22 April 2020.


110 Ibid.


114 Associate Professor Daniel Mohd. Yusof, International Islamic University, personal communication, 12 April 2020.


119 Focus group discussion with Malaysian undergraduates on 21 December 2019.


121 Priyank Mathur, a former Counterterrorism Officer for the US Department of Homeland Security and now with Mythos Labs, currently works with comedians writing on the subject of CVE. His collaboration with the East India Comedy group in India on a parody video entitled “I want to quit ISIS” garnered 500,000 views on YouTube in its first seven months.


123 Samuel2012, p. 32.


126 Through qualitative indicators seen through the feedback from students and undergraduates all over Malaysia after seeing the Arno Michaelis video.


128 Max Boon, the International Centre for Counter-Terrorism, The Hague. Available at: https://icct.nl/people/mr-max-boon-ma-associate-fellow/ accessed on 20 April 2020.


131 BBC, *Mothers of Jihadists.* BBC. Available at: https://www.bbc.co.uk/programmes/p02fg9g4 accessed on 20 April 2020.


133 Samuels 2014.


136 Samuel 2018a, pp. 113-123.

137 Defined as a place where individuals find their ideas supported and echoed by other like-minded individuals.


140 Taylor 2017.


142 Samuel 2018a, p. 124.


144 Lelo 2011.


146 Veenkamp, Ivo and Sara Zeiger 2015.


151 Ibid.


154 Dr. Ismail and Dr. Tan, University Putra Malaysia, personal communication, 15 November 2019.


156 Ibid.

157 Associate Professor Daniel Mohd Yusof, International Islamic University, personal communication, 12 February 2020.

158 Samuel, T.K. 2018b, p.49.
Bibliography


Ahmad Tajuddin bin Mohd Said, SEARCCT, Malaysia, personal communication, 20 April 2020.


Andrew Timothy William, personal communication, 22 April 2020.

Associate Professor Daniel Mohd Yusof, International Islamic University, personal communication, 12 February 2020.

Associate Professor Daniel Mohd Yusof, International Islamic University, personal communication, 12 April 2020.

Associate Professor Daniel Mohd Yusof, International Islamic University, personal communication, 12 February 2020.

Associate Professor Daniel Mohd Yusof, International Islamic University, personal communication, 12 February 2020.

Associate Professor Kumar Ramakrishna, Nanyang Technological University, personal communication, 23 January 2018.

Banlaoi, R.C., Youth as Victims and Perpetrators of Terrorism: The Philippine Case, Paper delivered at the International Conference on Youth and Terrorism organised by the Ministry of Information in collaboration with the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), Kuala Lumpur, Malaysia on 26 February 2009.


Dr. Ismail and Dr. Tan, University Putra Malaysia, personal communication, 15 November 2019


O’Malley, Brendan, Education Under Attack, a global study on targeted political and military violence against education staff, students, teachers, union and government officials, aid workers and institutions. Paris: UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000186809 accessed on 2 April 2020.


Professor Bilveer Singh, National University of Singapore, personal communication, 4 March 2018.

Professor Bilveer Singh, National University of Singapore, personal communication, 14 April 2020.


Ramakrishna, K., ‘There’s no such thing as non-violent extremism,’ TODAY, 18 August 2016. Available at: https://www.todayonline.com/commentary/theres-no-such-thing-non-violent-extremism accessed on 19 June 2020.


Toastmasters. Available at: https://www.toastmasters.org/ accessed on 22 April 2020.


Yayasan Sukarelawan (YSS)/Student Volunteers Foundation. Available at: https://sukarelawansiswa.my/ accessed on 22 April 2020.


Zan Azlee, journalist, personal communication, 8 November 2019.
Web-based Resources

The Forgiveness Project. Available at: https://www.crisisgroup.org/
Global Counterterrorism Forum (GCTF). Available at: https://www.thegetf.org/
Global Internet Forum to Counter Terrorism. Available at: https://www.gifct.org/partners/
Hedayah Centre. Available at: https://www.hedayahcenter.org/
IMAN Research. Available at: https://imanresearch.com/
Institute for Policy Analysis of Conflict. Available at:
http://www.understandingconflict.org/en.html
International Crisis Group. Available at: https://www.crisisgroup.org/
S. Rajaratnam School of International Studies (RSIS) Commentaries. Available at:
United Nations Office on Drugs and Crime (UNODC). Available at: https://www.unodc.org/
United Nations Office of Counter-Terrorism. Available at:
https://www.un.org/counterterrorism/
United Nations Counter-Terrorism Centre (UNCCT). Available at:
https://www.un.org/counterterrorism/cct
United Nations Educational, Scientific and Cultural Organisation (UNESCO). Available at:
https://en.unesco.org/
United Nations Interregional Crime and Justice Research Institute (UNICRI). Available at:
http://www.unicri.it/
Chapter 8
Prevention of Radicalization to Terrorism in Prisons: A Practical Guide
Gary Hill

This chapter focuses more on the practical than the theoretical. Much of the chapter will focus on how to identify inmates (and staff) at risk of becoming radicalized and how to work with them. In addition to looking at potential radical inmates, the chapter also deals with violent extremist offenders, who prison professionals often include when dealing with radical inmates. Why and how individuals become radicalized in prisons is explored. Many news articles, political presentations, and common knowledge indicate that prisons are “hotbeds for the recruitment of radicals” and that this is a big problem. Whether that is true is examined. The current emphasis on developing prison programs dealing with radicals are reviewed and summarized. The issue of whether radicalization in prisons is worthy of special programs or whether normal good prison practice would be just as effective is explored. Issues of dealing with inmates who enter the prison system already radicalized and who are possibly members of radical or terrorist organizations are explored, and the types of classification tools used to identify them are discussed. The chapter also looks at differing concepts as to how and where potential radicals should be housed. A major section of the chapter deals with the training of prison staff to identify and work with potential radicals. The use of “Dynamic Security” as a tool to help in the fight against prison radicalization is explained. Examples of various treatment models used in the rehabilitation of terrorists are presented. In its final section, the chapter offers general observations and recommendations for working with radicals, convicted terrorists and violent extremist prisoners.

Keywords: prisoners, corrections, radicalization, violent extremist, human rights, dynamic security, terrorist
“The terrorist enemy that threatens civilization today is unlike any we have ever known.”

“Prisons in Europe are becoming ‘breeding grounds’ for jihadist groups, with some criminals seeing violent extremism as a form of redemption for their crimes.”

“Ripe for radicalization: Federal prisons are ‘breeding ground’ for terrorists, say experts.”

Headlines, politicians, and pundits issue dire warnings – like those cited above - that appear to make a chapter on the prevention of radicalization to terrorism in prisons one of the most important criminal justice issues of our time. However, reality paints a different picture. First, terrorism, in all its forms, is not new. Groups with names like Viet Minh, Irgun and Stern Gang, National Liberation Front of Algeria, Palestine Liberation Organization (PLO), Irish Republican Army (IRA), West Germany’s Red Army Faction, Japan’s Red Army, Italy’s Red Brigades, and Ku Klux Klan indicate that terrorism has a long history all over the world.

The size of the problem of terrorists in prisons varies from country to country. In some places it is substantial: Israel has almost 6,500 terrorists in prison - but this is exceptionally high. In most countries, the numbers are small. Great Britain, for example, has nearly 150 terrorism-related inmates - out of a prison population of 85,000 convicted offenders. The US has under 450 individuals convicted of terrorist-related crimes - out of a total prison population of 1.5 million. By contrast about 200,000 gang members reside in US prisons.

In other words, in terms of the types of inmates that are of significant concern to prison officials, terrorist-related offenders are not a major factor. However, because of the vast damage a single terrorist can cause, recidivist terrorists are a major concern after release from prison. The notoriety of prisoners convicted of terrorist acts, especially where violence was involved, often forces prison officials to treat them as high security risks even when they are not. The problem of radicalization in prison needs to be seen in relation to wider incarceration problems. Security, programming, rehabilitation, humane treatment when dealing with radical and violent extremist inmates are not issues which have new meanings for most prison professionals.

Much of what follows comes from work began by this author in late 2016 while working with several national prison systems, organizations, and individual experts in attempting to develop training programs for staff who have to deal with radical, terrorist, and violent extremist inmates. A draft paper, entitled “Staff Training on Radicalization and Violent Extremist Inmates” was prepared by the author of this chapter and widely circulated to prison, security, and terrorism professionals. Their feedback was used to modify that draft and has led to the chapter presented here. Those who provided input are too numerous to list, but their contributions to this chapter are truly appreciated.

To ask why people become radicals or violent extremists is like asking why people become criminals. Though there is much research and even more theorizing, the important issue for those working in corrections - especially those on the front line who are in daily contact with inmates - is how to identify potential radicals and extremist violent offenders. Four issues stand out:

1. How can prison officials work with ideological offenders in such a way that corrections systems do not lose their ethical standards of humane treatment?
2. What can prison officials do to help divert such politically motivated inmates from engaging in acts of violence?
3. Can radicalized inmates be trusted in prison programs and can some of them be de-radicalized or at least disengaged from violent extremism once they are released?
4. Does the presence of radicalized inmates in prisons, on parole, or in community treatment centers, make the job of correction personnel more difficult and more dangerous?

Of major importance to all working in, or with, corrections, is to understand the offenders in their care and to treat them with dignity and respect. The task at hand is to ensure the safety of fellow staff, the inmates, and the public while the offenders are in the care of the correctional system. The job is also to ensure that staff actions do not make the offenders more dangerous. In addition to being the keepers of security within correctional institutions, staff are also responsible to help with inmate programming and preparation for release.

Definition of Terms

The editor of this Handbook, Alex P. Schmid, in this Handbook and other publications, has written extensively on the topic of defining terrorism and related terms. However, for purposes of this chapter, the following definitions are being used. These definitions might not be the most appropriate ones for all discussions on the topic. However, they are the ones used by those who reviewed and contributed to the work on which this chapter is based. In other words, these conceptualizations have proven useful for the purpose at hand.

Radicalization represents a dynamic process whereby an individual increasingly accepts and supports violent extremism. The reasons behind this process can be ideological, political, religious, social, economic, or personal.

Violent extremism consists of promoting, supporting, or committing acts of violence that may lead to terrorism and which are aimed at defending an ideology advocating racial, national, ethnic, or religious supremacy and/or opposing core democratic principles and values. "Terrorism" is defined in this chapter as conceptualized by the US’ Library of Congress Federal Research Division:

"Definitions of terrorism vary widely and are usually inadequate. Even terrorism researchers often neglect to define the term other than by citing the basic U.S. Department of State (1998) definition of terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.” Although an act of violence that is generally regarded in the United States as an act of terrorism may not be viewed so in another country, the type of violence that distinguishes terrorism from other types of violence, such as ordinary crime or a wartime military action, can still be defined in terms that might qualify as reasonably objective. Social science research defines a terrorist action as the calculated use of unexpected, shocking, and unlawful violence against noncombatants (including, in addition to civilians, off-duty military and security personnel in peaceful situations) and other symbolic targets, perpetrated by a clandestine member(s) of a subnational group or a clandestine agent(s) for the psychological purpose of publicizing a political or religious cause and/or intimidating or coercing a government(s) or civilian population into accepting demands on behalf of the cause.”

Terrorism Inmates are incarcerated persons who, as a result of being radicalized either prior to, or during, imprisonment, engage in some or all of the following activities:

- recruiting other prisoners;
- supporting extremist groups from prison;
- getting support from extremist groups outside prison;
• preparing for violent extremist/ideologically-inspired illegal acts after release;
• manifesting terrorist ideology-inspired hostility to other groups of prisoners and/or staff;
• increasing their radicalization level because of grievances/frustrations/anger related to being in prison.

Rehabilitation in this chapter is defined as the process where individuals or groups cease their involvement in organized violence and/or terrorism. The process can involve de-radicalization and/or disengagement. While de-radicalization aims for substantive changes in an individual’s ideology and attitude, disengagement concentrates on facilitating behavioral change. The disengaged terrorist may not be “de-radicalized” or repent at all. Often physical disengagement may not result in any concomitant change or reduction in ideological support.

Prisons and Corrections are used interchangeably in this chapter and mean one and the same. That is also true for the terms correctional staff and prison staff. Though most national governments, professionals, and research organizations have adopted the use of the term corrections, the laws of some states use the term prisons.

Prisoner Radicalization is defined by the US Department of Justice as “the process by which inmates who do not invite or plan overt terrorist acts adopt extreme views, including beliefs that violent measures need to be taken for political or religious purposes.” According to the same source, a distinction needs to be made between prisoner radicalization and terrorist recruitment, which means that inmates are solicited to engage in terrorist behaviour or commit terrorist acts - “the term prison radicalization usually refers to individuals being radicalised in prison, not that terrorist plots are being formulated in prison.”

Radicalization in Prisons

How Radical and Violent Extremist Offenders might Differ from “Normal” Inmates

While “ordinary” criminals commit crimes in pursuit of selfish and/or personal goals, politically motivated offenders believe that they are acting on behalf of a certain group, (a segment of) society, or humanity as a whole. Politically motivated offenders commonly distinguish between “legality” and “legitimacy,” arguing that breaking the law is justified when a particular policy or the entire political or legal system are illegitimate.

Potential Impact of Prison Experience on Radicalization

It is helpful to understand how the prison experience can contribute to certain inmates becoming radicalized. One also needs to realize that the prison experience can also affect staff. Here are three examples:

First, Dr. John Cacioppo, the late Director of the University of Chicago Center for Cognitive and Social Neuroscience, studied what he called “perceived social isolation.” One can feel isolated in a crowd. One can also choose to be alone and feel blissful solitude. When people feel others around them are threats rather than sources of cooperation and compassion, they feel socially isolated and lonely. Lonely people are often completely unaware that their brain has gone on alert. Lonely people are often hypersensitive to social threats. Lonely people, focused on self-preservation, take other people’s dire circumstances less seriously.

Second, Australian researchers, Elizabeth Mulcahy, Shannon Merrington, and Peter Bell described inmate vulnerability and its impact on radicalization as follows:

“When a person becomes imprisoned it is common for the individual to go through physical and emotional trauma that can make them more vulnerable to recruitment. For example, in the beginning when an individual is placed in jail, acute and chronic stress factors can give rise to physical problems (e.g. sleep disorders, loss of appetite, etc.) which can make the prisoner more
impressionable and vulnerable. At this moment a recruiter can enter into contact with the new prisoner and evaluate their vulnerability and likeliness to conform to their extremist group. It is also common for incarcerated individuals to undergo unbalanced emotional states, such as states of discontentment-excitement (hate, anger, doubt) and states of discontent-relation (humiliation, fear, sadness). This unbalanced emotional state is ideal for possible recruiters to infiltrate the minds of the vulnerable and impressionable… There are instances where an incarcerated person can lose their grip on their individual identity. This is most prominent in foreigners who are incarcerated in another country and who do not speak the language.\textsuperscript{6}

Third, the UK’s Prison Reform Trust, in assessing the potential for mental health damage a stay in prison can inflict,\textsuperscript{7} found that for the majority of prisoners, imprisonment was likely to have the following effects:

- isolation from families and social networks;
- austere surroundings, loss of privacy; poor physical and hygienic conditions;
- aggression, bullying, fear, suspicion and the attitudes of unsympathetic and uninformed staff;
- lack of purposeful activity, personal control, power to act and loss of identity;
- pressure to escape or to take drugs;
- shame and stigmatization;
- uncertainty, particularly among remand prisoners, and concern about re-integration into the outside world.

**Radicalization Occurs for Many Reasons and From Many Different Causes**

Root causes of radicalism are almost as varied as there are differing views among individuals on political, social, cultural, moral, religious or economic precepts. Religiously motivated terrorism accounts for only a part of all terrorism – at least in the West. According to the US Consortium for the Study of Terrorism and Responses to Terrorism (START)\textsuperscript{8}, between 1970 and 2011, 32 percent of the perpetrator groups were motivated by ethnonationalist/separatist agendas, 28 percent were motivated by single issues (such as animal rights or opposition to a war), and only seven percent were motivated by religious beliefs.

**Reasons for Joining a Terrorist Cause**

Lisa Andrews, writing in the Developmental Psychology Student Newsletter from Mesa Community College’s Psychology Department, concluded, “…. that every terrorist act has a specific, premeditated goal, with a predicted outcome.” The categories she identified were:

- Change: These acts of terrorism are motivated by the achievement of a goal. This goal may be related to social, religious, or political change;
- Religious: This group believes it is justified because of religious commands found in the Bible, Torah, Quran; they use these same religious beliefs to recruit more followers;
- Social: Other groups are motivated by purely social causes. Its object will be to overthrow not just governments, but the very economic and technological basis of contemporary societies;
• Political: The leaders of a given idea or social movement come together, in the form of a militia or rebel group, and bring about political change in order to rid society of an undesired ruling power;
• Revenge: There have been many instances where terrorism has been used as a means to avenge what is considered an unjust or offensive act;
• Attention: Terrorism has been used as an effective means of gaining the attention of the public, using fear.
• Symbolism: One thing that is important to acknowledge when speaking of terrorism is the importance of symbolism. Every terrorist act is designed to convey a specific message. Even randomly seeming terrorist acts seek to convey a basic message of fear: "We can get you anywhere, at any time. There is no one to protect you”.

Lisa Andrews further concluded that “most terrorists have several motives for committing terrorist acts and several, if not all, of those mentioned above can be used in order to try to explain their motives. The only true way to determine their motives is to ask the terrorists themselves.”

Anneli Botha, a researcher from the South African Institute for Security Studies, who studied radicalization, interviewed members of radical organizations in a number of countries. Using the results of one of her studies, it became clear that all did not join a violent group for the same reasons. She identified ten different motivational factors:

• Economic reasons;
• Religious and economic reasons;
• Religious reasons;
• Forced to join;
• Personal reasons;
• Religious and ethnic reasons;
• Religious reasons and forced to join;
• Religious and personal reasons;
• Economic reasons and desire for adventure;
• Desire for adventure.

Prison Considerations Specific to Radicalization and Violent Extremist Inmates

The information above provides some general background but needs to be modified or expanded for particular countries. It is good enough for a general understanding of radicalization, though far from comprehensive. It provides some information that educators, policy makers, and correctional administrators may find of interest and useful. Our concern in this chapter is for correction staff who are in direct contact with inmates: how can they identify inmates who might be vulnerable to, or are already engaged in, radical or violent extremist activities? And how can prison staff best interact with those inmates?

A. Inmate Classification (Risk and Needs Assessments)

Better managed prison systems utilize evidenced-based security classification instruments. Frank Porporino, a clinical psychologist and researcher with more than forty years of experience as a front-line practitioner, noted:

“What a Security Classification instrument allows you to do is capture both, some of the research informed factors related to potential for escape and/or violence (e.g., age, history of violence) and then marry those with some important ‘correctional policy’ factors where some level of caution
is needed in inmate classification even if the research doesn’t suggest that these factors are clearly predictive (e.g., sentence length, severity of the offence, time left to serve, and even history of prior escapes).”

If correctional staff are going to work with inmates who may be violent extremist inmates or radical inmates, or in danger of being radicalized, the more information they have about the inmates in their care, the better they can do their job. At the same time, staff should know the factors that are included in evidenced-based risk and needs assessment instruments so they can provide feedback to the classification staff. The classification process is not a one-shot operation. It is a continuing process that is constantly reviewed and updated to reflect changes in the inmates. Thus, constant and consistent input from line staff is very important.

According to the European Radicalisation Awareness Network (RAN)’s Prison & Probation Working Group, the following recommendations should be considered for a radicalization-focused risk assessment:

1. Invest in, develop, and offer general awareness training to all staff;
2. Develop a two-step risk assessment procedure in cases of potential radicalization;
3. Base assessments on multiple sources of information to increase reliability;
4. Give peer and management support to practitioners carrying out risk assessments;
5. Avoid labelling by having continuous cycles of risk assessment;
6. Run a well-organised, orderly prison is a key prerequisite to avoiding further criminalisation as well as radicalization;
7. Choose among different prison regime: [prisoner] concentration, dispersal or combinations.

B. Should Persons Convicted of Acts of Violent Extremism be Placed in the General Prison Population or kept Separately?

The following table contains a short analysis of the advantages and disadvantages concerning three types of prison regimes. It is important to emphasize that more extensive knowledge about these regimes and how they are organized is necessary to further inform the debate on prison regimes.

<table>
<thead>
<tr>
<th>Regime Choice</th>
<th>Potential Advantages</th>
<th>Potential Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Dispersed</td>
<td>• Prisoners are less likely to regard themselves as marginalized because of their beliefs. They will, to some extent, be treated as ordinary prisoners; • Prisoners might be positively influenced by being around different groups of prisoners with different mindsets.</td>
<td>• Handled by generalist staff members instead of specialists; • Risk of radicalizing other prisoners; • Both the prisoner and their environment require close monitoring to identify any negative influences; • Risk of extremists mingling with criminal networks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regime Choice</th>
<th>Potential Advantages</th>
<th>Potential Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Concentrated,</td>
<td>• Prisoners are more likely to regard themselves as marginalized because of their beliefs. They will, to some extent, be treated as ordinary prisoners; • Prisoners might be negatively influenced by being around different groups of prisoners with different mindsets.</td>
<td>• Handled by specialist staff members; • Risk of radicalizing other prisoners; • Both the prisoner and their environment require close monitoring to identify any positive influences; • Risk of extremists mingling with criminal networks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regime Choice</th>
<th>Potential Advantages</th>
<th>Potential Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Combination</td>
<td>• Prisoners are somewhere in between the two above models;</td>
<td>• Handled by mixed staff members; • Risk of radicalizing other prisoners; • Both the prisoner and their environment require close monitoring to identify any positive and negative influences; • Risk of extremists mingling with criminal networks.</td>
</tr>
</tbody>
</table>

Table 1. Housing of Radical - Dispersed, Concentrated, Combination Potential Advantages & Disadvantages
### 2. Concentrated/Placed Together

| People suspected or convicted of violent extremist acts are placed together in a separate terrorist wing. | • All the prisoners on a terrorist wing can be fully monitored by their contacts within the wing;  
• Limited opportunity to influence other prisoners;  
• Individual and group work with prisoners on deradicalization/disengagement and other interventions;  
• Staff on a terrorist wing become experts because they work with radicalized prisoners on a daily basis; only a small group of staff members must be trained;  
• This approach may reassure the public that real and powerful measures are being taken to safeguard society. | • The terrorist wing can facilitate further radicalization/extremist acts. New bonds between extremist prisoners can be formed and this can increase the risk of plotting attacks when they leave prison;  
• Lack of contact can cause difficulties when socialising someone after their release;  
• Perceptions of unfairness could lead to further radicalization of the prisoner, but also of supporters outside the prison;  
• Such facilities are expensive need capacity for urgent situations;  
• Prisoners might feel stigmatized by being in a separate wing, yet others see it as a sign of raised status or credibility as an extremist. It could therefore lead to greater cohesion within the group.  
• Deradicalization/disengagement interventions could be hampered;  
• The approach risks establishing a group with great symbolic power. |

### 3. Combination

| Based on a risk assessment, it is decided whether to place a person suspected or convicted of violent extremist acts in a separate or an ordinary regime. | • Tailor-made approach that fits the risk and needs of the prisoner;  
• After screening and assessment, the detainee can be placed in the most appropriate regime. | • Both regimes need to be available;  
• Need for robust assessment tools. |

### 4. Individual Separation or Transfer to Another Institution

| This is not part of the RAN P&P but worthy of consideration when appropriate. | • Housing in a special housing unit for limited amounts of time to diffuse a potentially dangerous situation can be a helpful security tool.  
• But note: its use must be carefully monitored and allow for frequent human contact on a daily basis.  
• Transfer to another facility should be tied to the needs and risk assessment along with consultation from security staff. | • Does not help inmates in terms of programming and, if not handled in a fair and consistent manner, can be harmful to the institutional mission and give an inappropriate message to staff in terms of working with inmates. |
Human Rights Considerations in the Incarceration of Radical and Violent Extremist Offenders

*Respect for Human Rights and Fundamental Freedoms*  
While terrorists usually violate both humanitarian law (their acts are akin to war crimes) and human rights law (e.g. the right to life), they still ought to be treated with respect, based on the laws of the land. In particular, three points need to be kept in mind.

First, preventing and tackling radicalization and violent extremism shall always be based on the rule of law and shall comply with international human rights standards because respect for human rights and the rule of law is an essential part of a successful counter-radicalization effort. Failure to comply with these is one of the factors which may contribute to increased radicalization.

Second, torture and inhuman or degrading treatment or punishment is prohibited. Freedom of expression and freedom of religion shall be respected. Prison officers ought to review the lessons they have received in their basic training on international standards. They all apply to radical and violent extremist offenders as well.

Third, it is possible that some extra restrictions may be placed on some radical and violent extremist offenders, based on their behavior, risk assessment, and classification. Therefore, punitive measures, use of force, and means of restraint shall be proportionate to the direct and serious threats of disruption of good order, safety, and security in a given prison in order to preserve, to the extent possible, relations of trust and support in helping the reintegration of offenders.

By treating terrorists and those attracted to terrorism on the basis of more humane standards than terrorists treat their prisoners and adversaries, the good example might, hopefully, rub off — at least to some extent. Treating unkind persons with kindness generally produces better results than treating them likewise or worse.

Behavioral Factors that may Indicate an Individual is Becoming Radicalized

Indicators are meant as potential warning signs and should be communicated to intelligence and supervisory staff. If deemed important by supervisory staff, the correctional officer(s) may be asked to look for specific behaviors when interacting with the inmate in question. However, it should be noted that many of the following signs are the same a correctional officer should look for to identify an inmate’s potential vulnerability to escape, violence, mental health issues, and suicide. Thus, normal staff training on these subjects ought to include early warning indicators of terrorism and radicalization as well.

*Indicators of Radicalization in Inmates*

- The individual abruptly abandons friends and family members;
- On those increasingly rare occasions where such inmates do see their family, they berate them for their supposedly impious behavior;
- They stop participating in activities that used to occupy a lot of their time - such as sports or group activities/associations;
- They believe they have found the true path to religious enlightenment and anyone else who does not follow it is of less worth;
- They often exhibit growing hatred and intolerance towards others who do not adhere to their beliefs (these can be of a political, social, cultural, or religious nature);
In terms of hatred and intolerance of beliefs of a religious nature, this includes rejecting fellow Muslims, Jewish, or Christians of different denominations, as well as religious leaders who repudiate violence;
- They refuse to engage with, or debate, ideas that counter their own;
- They turn their back on their life as it was before radicalization;
- Individual changes in appearance include: beard, clothing, gang signs;
- They develop obsessive patterns of behavior and they look out for martyrdom and the apocalypse;
- They avoid other inmates;
- They speak in admiration of terrorists or terrorist acts;
- They participate with members of terrorist or radical groups;
- They begin physical training such as body building;
- They avoid contact with staff;
- They donate money to groups with radical beliefs or leaders;
- They request transfer to another wing;
- They request special food;
- They increase the number of appeals and legal filings;
- They increase contact with human rights groups and other NGOs.

Indicators of a group of inmates possibly forming an organization (formal or informal):
- The group seeks self-government or control of its members;
- The group starts a joint canteen account (either formally or informally);
- The group establishes strict discipline for its members (regarding talking to staff without permission of the group leaders, assigning punishments for violation of group protocol, etc.);
- The group accepts leadership and direction from outside organizations or individuals;
- The group tries to control the work assignments of their members;
- The group appoints a speaker for the group (individuals are no longer allowed to talk to staff on their own);
- The group organizes classes on ideology, languages, “how to” on skills that could be useful to terrorists;
- The group establishes joint prayer sessions;
- The group attempts to communicate with inmates of other prisons;
- The group begins to contact non-group inmates to increase group appeal, resources, or influence;
- The group increases contact with NGOs, lawyers, legislators, or others.

Again, one should remember that none of these signs are by themselves firm proof of radicalization. They are, however, potential signs and should be considered in conjunction with other behaviors. Nevertheless, from a correction officer’s standpoint, if one is not sure, the best rule is “if you see something, say something.” Correction officers should let the prison intelligence team know and also make sure the staff coming on to the next shift are informed about their observations of suspicious behaviour and reasons for concern.
Special Security

Personal Safety

Safety is a top priority for corrections. While at work, staff are taught procedures and approaches that are designed to keep them safe while they manage offenders, including radical and violent extremist offenders. Treating everyone, including offenders, with dignity and respect will go a long way to ensuring everyone will stay safe. Most corrections staff go about life without fear or concern. Most staff will never have any problems. However, the fact remains that some offenders may be threatening or dangerous. They, or their associates, may threaten staff, or may try to get personal information – such as home addresses – for criminal purposes. All staff must be taught, it is not ok for anyone to threaten them. If they are threatened, they must report it to their supervisor – even if they do not believe the person will carry out the threat. Not all staff will want or need to take all the steps listed below. It is about assessing the risk and taking what action is sensible.

Correction guidelines recommend that staff who work directly with offenders keep their information as private as possible as a precautionary measure. What follows will help staff to safeguard their personal information; think about ‘common sense’ security of themselves and their family; and take the right action if threatened.

Protecting Personal Information

- Private information should stay private. Remind staff in training that when they are at work, offenders may be present. They should not discuss anything private about themselves or others if an offender could be listening. If they must discuss something private, close the door;
- Think about written information as well – could an offender see anything in a staff’s private bag or on their computer screen? Lock private files away and lock the computer screen when away from the duty station. Be careful what is put in the rubbish bin;
- Don’t give any information to an offender or member of the public who asks for private details or those of a colleague (things like cell phone number or home address).

Staff should always know who they are talking to on the phone. Officers should check that the person they are talking to really is who they say they are – especially if they are asking for private information about another staff member or offender. For example, if they receive a call from a person claiming to be a police officer, rather than give them the information directly, the staff person should call the police station and ask to be put through to the person who called them.

Social Media – A Sample Personal Checklist:

- Do not post anything that shows you work for corrections;
- Do not post personal information such as date of birth, maiden names, names, and details of children;
- Think carefully before accepting friend requests; Use privacy controls on sites like Facebook so that only approved users can view your page. You can usually restrict who can share information and photos you have posted to your page so other users cannot forward your information;
• Think carefully before disclosing information on your social media account(s). There is no guarantee of privacy, even with tight security settings. Anything you put on a social media platform can be cut, pasted, and sent simply by taking a screenshot.
• Avoid tagging people in photos you have uploaded. Photos are often tagged so that the names of the people in the photo are visible;
• Avoid checking in at locations on your social media account(s). When using social networking on smart devices such as iPhones or iPads, users can check in at locations, which simply shows where they are. This information could be used to track down that user by criminals;
• Consider the implications of uploading photos to your social media account(s). Photos taken on smart devices are often geo-tagged (geographical data is imprinted into the photo properties which shows where the photo was taken). When these photos are uploaded to social networking sites, this data often remains. If a user has uploaded a photo of their house or vegetable garden, for example, others could potentially use the geo-data embedded in the photo to obtain the user’s home address;
• Talk to your family – especially children – about ways to stay safe online.

Security at Work – A Sample Personal Checklist:
• Know your colleagues. It is important to ensure that any strangers who gains access to a corrections site can easily be identified;
• Beware of “ghosting” – when a person follows behind a staff member and gains access to secure areas by slipping through gates or doors before they close;
• On a large site, it is impossible to know everyone, so stay alert and if you see someone unfamiliar check that he/she has a visible and valid ID card. All staff are allowed to challenge an unknown person and ask to see proof that they are allowed to be there – but make sure it’s safe to do so. If you are alone you should call for back-up or find a colleague before you challenge someone.

Security Outside of work – A Sample Personal Checklist:
• Tell someone where you are going and when you will be back;
• If you are walking at night, stay on brightly lit, well-used streets as much as possible;
• If you must take a poorly lit route, walk near the curb or well away from shrubbery, dark doorways and other places allowing concealment. Be alert and avoid ‘short cuts’ through dark alleys or deserted parks;
• If taking your car, do not leave anything on view that could associate you with corrections;
• Park in well-lit areas and always close your car windows and lock the doors.

Security at Home – A Sample Personal Checklist:
All families should have a safety plan, which specifies what everyone will do in an emergency. This is also good to have in case of a natural disaster, such as an earthquake. Every plan will be unique to the circumstances, but the following are some of the things to include or consider:
• What will each of you do in the event of an emergency?
• How and where will you meet up in the event that home is no longer safe?
• How will you contact each other in cases of an emergency? If you cannot contact someone, who or where will you leave a message?
• What will you need to do for members of the household with a disability or special requirements?
• What needs to be done for pets, domestic animals, or livestock if the home is no longer safe?
• Who will be responsible for collecting children from school if you need to relocate in haste?
• Who could help you or where could you go if you need to relocate in a short amount of time?

Home Security
• Always check who is at the door before opening it – consider having a door chain or security peep-hole installed and never open the door if you are suspicious in any way;
• After dark, close the curtains so people cannot look into the house;
• Check all doors and windows are secure before going to bed, or leaving the house (even if you are only leaving for a few minutes) or going to a different part of the house;
• Keep a strong “courtesy” light by the front and back door on at night – it could be operated by a motion sensor;
• If you go out at night, prepare your return by turning on outside lights. Some inside lights should also be left on;
• Keep track of your house keys and never leave one outside in an obvious place (such as under a mat or in a mailbox);
• Arrange for fixed times for workmen to call – check their identity and never leave them in the house on their own;
• Check parcels/deliveries before accepting them;
• Trim bushes or trees that are close to the house;
• Talk to children and teenagers about staying safe (e.g., how to open the door or answer the phone).

If You See Something You Think is Suspicious:
• Report to police any suspicious vehicle or people loitering near your home. Before you do so, get as much information as possible, such as:
• Description of the individual and what they are doing;
• Description of the car including make, color and registration number;
• If you see something, if you hear something, if you suspect something - say something.

Telephone Security – A Sample Personal Checklist:
• Be wary about giving personal information out on the phone, especially if you do not know the caller. It is better to take a name and number and call back if you are suspicious in any way.
• Make sure children and other family members know how to be careful when answering the phone.
Anonymous calls and telephone threats are usually intended to lower your morale. Your natural reaction when hearing a hostile voice is one of anger/fear and to cut off the conversation. However, the caller may provide clues to their intentions or specific threats and, if possible, you should try to keep them talking:

- Try to identify the voice by age, sex, accent, peculiarities, etc.
- Listen for background noise, which may provide valuable information, e.g., music, machinery, animals, industrial noises, railway station sounds, etc.
- Write down the details of the call immediately.
- Contact the police without delay.

**Institutional Security in and Around Prison**

Tower, Gate, Perimeter and Transportation Security Personnel should constantly ask themselves “are people watching the facility or posing a threat to facility personnel?”

- They must watch not only visitors, inmates, and vendors but also others who are outside the facility.
- Surveillance of your facility or activities.
  - If you see more than one unexplained/suspicious sighting: ask yourself if it is a coincidence or a potential problem.
  - If you note three or more unexplained/suspicious sightings: assume hostile surveillance until otherwise explained
- Note especially individuals taking pictures, sketching, or note-taking.

**Inmate Work and Recreation Areas (especially if there are suspected radical and/or violent extremist offenders involved):**

- Be especially vigilant in searches of individuals, equipment, tools, and products. Follow procedures without variation;
- Follow the tool control protocol rigidly to ensure no tools or work items are taken outside of the prisoners’ work area;
- Be close enough to inmates to observe them and hear conversations, but position yourself to be prepared in case of an unprovoked attack. Remember the motivation of potential radicals and violent extremist inmates. In addition to being a potential danger to staff and other inmates if they are provoked or frightened or upset, some may launch an unprovoked attack as a part of their radical ideology;
- Be aware of signs indicating a possible organized attack. Changes in normal habits or dress may provide clues. Any abnormal behavior by a group of inmates should be assumed to be hostile until proven otherwise. Examples might be inmates wrapping their bodies with newspapers or magazines under their shirts to serve as homemade body armor or inmates who normally wear sandals in the yard switching to wearing shoes for better protection or mobility.

**Dynamic Security**

The best weapon in the fight against radicalization of prisoners and violent extremist inmates is well trained staff – especially staff using Dynamic Security. Dynamic Security is a concept and a working method by which staff prioritize the start and maintenance of everyday communication and interaction with prisoners, based on professional ethics. It aims at better
understanding prisoners and assessing the risks they may pose as well as ensuring safety, security, and good order, contributing to rehabilitation and preparation for release. This concept should be understood within a broader notion of security which also comprises structural, organizational and static security (walls, barriers, locks, lighting, and equipment used to restrain prisoners if necessary). The concept of Dynamic Security is based on:

- positive relationships, communication, and interaction between the staff and prisoners;
- professionalism;
- collecting relevant information;
- insight into, and improving social climate of, the penal institution;
- firmness and fairness;
- understanding of the personal situation of the prisoner;
- communication, positive relations, and exchange of information among all employees.

Dynamic Security involves knowing what is going on in a prison, in addition to providing a safe and secure background against which the whole range of activity making up the life of a prison takes place. The concept of Dynamic Security has the benefit of engaging prisoners individually and gaining both material and intuitive insights into the operation of the prison. When implemented effectively, Dynamic Security allows prisoners to feel comfortable when approaching prison staff before problems escalate. It is important, therefore, that staff take every opportunity to interact directly with prisoners and avoid retreating behind doors, into corridors or offices and stations unless required to do so.

Dynamic Security occurs when corrections officers interact and engage with prisoners while regularly walking through the area in which they are posted:

- Talking to prisoners, gaining their trust, and building rapport;
- Checking prisoners’ physical welfare during musters and head checks;
- Maintaining a consistent approach to inappropriate behaviour;
- Encouraging positive behaviour and addressing negative behaviour;
- Engaging in case management process;
- Following up on requests in a timely manner; and
- Remaining calm during incidents.

**Self-Assessment for Staff on the use of Dynamic Security**

- Competence: You’re good at what you do and you have the skills and knowledge that enable you to do your job well;
- Reliability: People can depend on you to show up on time, submit your work when it is due, and follow through on promises;
- Honesty: You tell the truth and are upfront about how things are;
- Integrity: You are known for your principles;
- Respect for others: Treating all people so that they feel that they really matter to you is part of your approach;
- Self-upgrading: Rather than letting your skills or knowledge become outdated, you seek out ways of staying up-to-date;
- Being positive. Having an upbeat attitude and trying to be a problem-solver makes a big difference to you;
Supporting others: You share the spotlight with colleagues, take time to show others how to do things properly, and lend them an ear when necessary. You do not criticize colleagues in front of inmates;

Staying work-focused: You do not let your private life needlessly impact on your job, and you do not spend time at work attending to personal matters;

Listening carefully: People want to be heard, so you give people a chance to explain their thoughts and feelings properly.

Placing the emphasis on the need for prison staff to establish positive relationships with prisoners is key to Dynamic Security. This concept rests on the notion that engaging with prisoners and getting to know them can enable staff to anticipate and better prepare themselves to respond effectively to any incident that may threaten the security of the prison and the safety of staff and prisoners.

Correctional Officers’ Role in the use of Dynamic Security:

- Guide and support, not push and demand.
- Let inmates be as independent as security allows.
- Remember inmates are always watching.
- Never be mean, spiteful, or belittle inmates (or fellow staff).
- Show inmates you care about them every day.
- Acknowledge when you make mistakes and apologize.
- Discipline, not punish.
- Look at what the inmate needs, not at what you want them to be.
- Know what the inmates are doing and with whom.
- Connect with the inmates every day.
- Talk and listen.

The nature of relations between staff and prisoners is also key to the concept of Dynamic Security. For example, the way in which prison staff address prisoners, how searches are carried out and their frequency, whether prisoners’ privacy is respected when they are required to remove clothing, whether restraints are used unnecessarily and in a way which is humiliating, whether privacy in toilets and showers is respected, whether prisoners are required to wear specially marked uniforms – these are all ways in which prisoners’ humanity and dignity may or may not be respected. Using disrespectful language, or subjecting prisoners to humiliating routines or practices without any security justification, constitute breaches of their fundamental right to be treated with humanity and with respect for their inherent dignity.

Unit Management

For unit management, a prison is broken down into defined units, each of which may contain a number of prisoner accommodation sections and static posts. Multi-disciplinary teams consist of disciplinary officials, educationalists, social workers, psychologists, religious care workers, and nurses who all deliver services in each defined unit. Individual team members have a responsibility for both security and prisoner development outcomes and are expected to develop constructive relationships with prisoners.

Benefits Associated with Direct Supervision and Unit Management
A member of staff (case officer) is assigned to specific prisoners and serves as the primary contact point between prisoners and the administration. This is done to:

- Increase the quality of relationships between prisoners and staff;
- Better communication and program planning;
- Increase program flexibility;
- Make decisions about prisoners being made more quickly by people on lower levels – those who really know them;
- Conduct more effective observation of prisoner activities resulting in early detection of problems for timely intervention;
- Ensure good quality information is received from, and about, prisoners which can be used to prevent escapes and control problems;
- Ensure development of correctional and managerial skills of staff;
- Utilize a multidisciplinary team to improve cooperation between staff from various disciplines;
- Develop an improved and more coordinated approach to rehabilitation and development programs.

Direct supervision and unit management are inextricably connected. Unit management staff members serve important and dual roles in security and programs. They “walk and talk” to prisoners and familiarize themselves with their personalities and identify their concerns.

**Prison Intelligence = Information + Analysis**

Intelligence within the prison context can be defined as follows:

- The prison intelligence function seeks, through objective strategic and operationally driven planned information and data collection, to identify those prisoners, visitors, staff and organizations planning to engage in activity, or who are engaged in an activity that may be a threat to the good order, safety and security of a prison before a negative/harmful/destructive event occurs.

The purpose of intelligence gathering on prisoners while in custody is not for the state to “spy” on them or to infringe on their basic human rights, but to ensure that they do not continue to commit criminal offences while in custody. By developing prison intelligence, the prison administration is endeavoring to make the custodial environment as safe and secure as possible for staff, the prisoners themselves, and ultimately the wider community. Due to the sensitive nature of prison information and intelligence (especially with regard to possible staff corruption), those chosen to work in this area need to have higher credentials in terms of integrity than in some other prison roles. Staff working in intelligence units are therefore sometimes subjected to enhanced security vetting that investigates their background and assesses the risk that they may pose.

It is important to remember that prison intelligence should be part of a broader law enforcement intelligence system. The volume and quality of information exchanged, and the speed with which requests are answered, will be indicative of the level of cooperation. Prison intelligence can also be vital to law enforcement operations outside prison. Similarly, intelligence from outside law enforcement agencies can be very important to understand what is happening in prison.
The Use of Informants or Human Sources for Gathering Intelligence

While informants may provide information that may not otherwise be available to prison management, the use of informants in prison is particularly dangerous for the informant and is also open to possible abuse. Informants may have many different motivations. They may, on the one hand, be prisoners seeking rewards (financial or early release), or, on the other, hardened criminals seeking to oust their opponents.

Importance of Prison Staff in Information Collection

Prison staff should gather information by always being vigilant and by reporting anything out of the ordinary by:

- Overhearing a conversation;
- Watching what prisoners do;
- Observing whom prisoners talk to - patterns of association;
- Looking out for patterns of behaviour and frequent actions;
- Identifying unusual activity or predictors of disruptive behaviour;
- Watching for physical changes (obscured views due to placing of physical objects in the line of sight);
- Observations during searching - hoarding of goods and clothes;
- Unusual requests or incidents.

Reporting should be done with the help of a Security/Intelligence Reporting Form (for a sample, see Appendix I).

Inmate Rehabilitation and Reintegration Programming for Radical and Violent Extremist Offenders

Programs to rehabilitate and de-radicalize terrorists are in operation in many countries, including Saudi Arabia, Afghanistan, Algeria, Canada, Egypt, Indonesia, Iraq, Jordan, Malaysia, the Netherlands, Nigeria, Pakistan, Philippines, Singapore, Spain, Sweden, the UK, the US, and Yemen. Such programs vary in terms of methods, support, and funding. For example, some countries (e.g., Egypt, Algeria, Israel) look at terrorists as a group whereas other countries (e.g., Saudi Arabia, Singapore, Afghanistan) work with imprisoned terrorists on an individual basis. Another difference between correctional systems is whether to separate violent extremists from other inmates or to integrate them. Israel has separate prisons or wings designated for “security prisoners”. The Netherlands has a “terrorism wing” in its Vught high security prison for a small number of inmates classified as terrorists, whereas the UK and Spain disperse their terrorist prisoners and place them in any of their high security prisons (see for four examples: Appendix II).

Final Observations and Conclusions

While approaches in various countries differ, the program presented here provides a general approach which has gained a following in the prison systems of those countries this author worked with. New programs and variations of these continue to emerge as new evidence-based findings are published and are positively received.

Based on this author’s experience as well as the research of others, what follows are some generally accepted conclusions:
• Prisons matter. Prisons have played an enormous role in the narratives of nearly every extremist and militant movement in recent years. Prisons are “places of vulnerability” in which radicalization can and does take place. Yet - and this should not be forgotten – some prison systems have also served as incubators for rehabilitation and peaceful transformations.

• Much of the current discourse about prisons and radicalization is negative. Yet prisons are not just risky places – they can play a positive role in tackling problems of radicalization and terrorism in society as a whole. Prisons can and should become net contributors to the fight against terrorism.

• Terrorists are not “ordinary” offenders. They often use their time in prison to radicalize other prisoners and mobilize outside support, and – when given the opportunity – will attempt to (re-) establish operational command structures.

• There are no hard and fast rules about whether terrorist prisoners should be concentrated together or separated from the rest of the prison population. Most of the countries practice a policy of dispersal and (partial) concentration, which distributes terrorists among a small number of high security prisons. Even within such mixed regimes, however, it is rarely a good idea to bring together leaders with followers and mix ideologues with hangers-on.

• The “security first” approach of many countries results in missed opportunities to promote reform. Many prison services seem to believe that the imperatives of security and reform are incompatible. In many cases, however, demands for security and reform are more likely to complement rather than contradict each other.

• Dynamic Security is an important and effective tool assisting prison staff to recognize inmates who are vulnerable to radicalization. It can contribute to keep them from becoming violent extremist inmates or from them joining terrorist organizations while still in prison or upon release.

Only with practice and experience will a prison officer gain the ability to be proficient in working with inmates in a respectful and effective way. The ability to spot signs of potential radicalization in an inmate is not easy nor is detecting the relevant cues an exact science. It takes full-time observation, good listening skills, communications with fellow prison staff and, last but not least, consistent adherence to good prison practice.

Gary Hill is the chief executive officer of CEGA Services in Lincoln, Nebraska (USA) and president of Contact Center, Inc., a private, nonprofit, international information and referral clearinghouse working in the areas of human services, criminal justice and illiteracy. Hill has been working in the field of corrections since 1964 and is the recipient of the American Correctional Association’s highest award. On special assignment to United Nations organizations, he has drafted more than forty training manuals in support of formal training programs for prison workers. Gary Hill is the Staff Training and Development Director of the International Corrections and Prisons Association (ICPA) and works with several Institutes of the United Nations Crime Prevention and Criminal Justice Program. He served on the United Nations Committee of Experts which prepared the update of the United Nations Standards for the Treatment of Offenders (the Mandela Rules) and the development of the standards for female offenders (the Bangkok Rules). For the Best Practices Unit of the United Nations Office of Peacekeeping Operations, Gary Hill reviewed the corrections activities associated with UN Peacekeeping and prepared a “Lessons Learned” document and a guidebook for use in future missions. He serves as an expert on three Council of Europe projects dealing with prison radicalization.
Appendix I: Sample Security/Intelligence Information Reporting Forms

**TEMPLATE EXAMPLE**
[XXXX] Prison Service

**SECURITY INFORMATION REPORT**

<table>
<thead>
<tr>
<th>Prison:</th>
<th>SIR number/year</th>
<th>Security Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Action immediately (Tick) □

☐ Inform Headquarters sign additional information and write what was reported (Tick)

Prisoner(s) name(s):

Prisoner(s) number(s):

Incident location:

Subject heading:

SECTION 1. Content of report

(Continue on a separate piece of paper if required)
Information submitted by (print name):

Date submitted:                  Time submitted:

Signature:

SECTION 2.  SIR received in intelligence Office by:

Name (print):

Date:                           Time:

Signature:

<table>
<thead>
<tr>
<th>Source</th>
<th>Information</th>
<th>Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Completely reliable</td>
<td>1. Report confirmed</td>
<td>1. Dissemination permitted within law enforcement agencies in the country of origin.</td>
</tr>
<tr>
<td>B. Usually reliable</td>
<td>2. Probably true report</td>
<td>2. Dissemination permitted to other national agencies.</td>
</tr>
<tr>
<td>E. Unreliable</td>
<td>5. Improbable report</td>
<td>5. Permits dissemination, but receiving agency to observe the conditions specified.</td>
</tr>
</tbody>
</table>

Evaluation (completed by Intelligence Office)
### SECTION 4. Head of Intelligence/Security

**Action(s) approved** (Tick if approved) □

If not approved then write alternative or additional action to be taken.

Name (Print): [Blank]
Signature: [Blank]
Date: [Blank]
Time: [Blank]

### SECTION 5. Prison Director (Officer-in-Charge)

**Final decision or comments**

(Specify if Headquarters was informed and what information was reported.)

Name (Print): [Blank]
Signature: [Blank]
Date: [Blank]
Time: [Blank]
Appendix II: Sample of Countries with De-Radicalization Programs

**Saudi Arabia**

A comprehensive counseling/education program is the heart of the Saudi program “designed to combat the intellectual and ideological justification for violent extremism”. The program uses intensive religious debates and psychological counseling. It is based on the belief that those recruited by terrorist groups often have little formal religious education. While they are in prison, they are encouraged to discuss and debate Islamic law with sheiks and scholars. This type of religious counseling seeks to correct the detainees’ interpretation of Islam through open dialogue.20

While the program begins in prison, it continues at the Care Rehabilitation Center, located in a former resort, just outside the capital city of Riyadh. A stay at the Center lasts up to six months and the prisoners participate in a wide variety of activities from Qur’anic studies to art therapy. There is a swimming pool on the grounds and there are also opportunities for other recreational activities. The correctional staff do not wear uniforms and inmates have 24-hour access to telephones. After leaving the Care Rehabilitation Center, the Saudi government monitors the progress of the inmates and offers support. Christopher Boucek wrote in a study for the Carnegie Endowment for International Peace, noting that “once an individual satisfactorily renounced his previous beliefs, assistance is provided in locating a job, and receiving other benefits, including additional government stipends, a car, and an apartment. Success of the program . . . is based in part on the recognition that being a radical is not inherently a bad thing. Acting on radical beliefs with violence, however, is, and that it is the behavior that needs to be modified.”21

The Saudi government initially claimed de-radicalization success rates of 80%. However, there were also many failures. One case that made the news was Mohamed al-Awfi who, after six years of detention in Guantanamo Bay by the US, was released to Saudi Arabia, and entered the Center’s program, taking classes in anger management, Islamic law, history and art therapy. Awfi claimed that he was tortured and mistreated during his time in Guantanamo. Shortly after his release from the Center, Awfi decided to take revenge on the United States and fled to Yemen. Saudi officials visited Awfi’s family and instead of threatening them, the officials told the family that they did not hate Awfi, only his behavior and though he made a mistake by running to Yemen, if he came back he would receive help. The family began to call Awfi in Yemen and not long after Awfi turned himself in. The Saudi’s “soft” approach to the rehabilitation of terrorists has been copied by other countries, but few have equaled the Saudi’s in terms of investment of time, manpower and money.

**Egypt**

Unlike the Saudi program that was initiated by the government after 9/11, Egypt’s program of terrorist rehabilitation began already in May 1997. At that time, the leadership of a-Gama’a al-Islamiya22 took the initiative to denounce the use of violence in jihad (except for self-defense). In November 2007, al-Jihad al-Islamiya adopted the de-radicalization model established by a-Gama’a al-Islamiya. Although the Egyptian security authorities were initially skeptical and hesitant to support the inmate-initiated program, they later came to accept and support it. The leadership of a-Gama’a al-Islamiya, after consulting with Islamic scholars from Al-Azhar University, released 25 volumes of revisions to their initial doctrines, entitled Tashih al-Mafahim [Corrections of Concepts]. The revisions included the recognition that Islam does not permit killing or terrorizing non-Muslim civilians and discussed the dangers that Al-Qaeda poses to Muslims worldwide.24
Iraq

The Munasaha program began on 9 March 2011, with the aim to rehabilitate prisoners in Anbar and Baghdad. Much like the Saudi program, it was designed to educate inmates about the damage terrorism caused to Iraqi society and was meant to make them realize that terrorism violates the law and is considered a sin by all religions. Previously, Task Force 134, the US unit charged with overseeing coalition detainee operations in Iraq, utilized an approach of segregating extremists, nurturing moderates and ensuring good care and custody for each detainee. Beginning with a classification process to separate recruiters from other inmates, the program included religious discussions conducted by US-vetted Iraqi imams, basic literacy education, and work programs. According to US authorities, the education component was particularly effective.

Singapore

With 16% of its prison inmates being Muslims, Singapore established the Religious Rehabilitation Group (RRG) to de-radicalize jihadi terrorists. Nearly 40 Islamic scholars and religious leaders make up a group dedicated to “deprogramming” detainees. By approaching the jihadists on religious terms, the RRG seeks to treat the problem at its root. As one security officer explained, “once you take an oath to God, it will take another man of God to undo it.”

Singapore is also home to the Behavioural Sciences Unit’s (BSU), Home Team Academy, which conducts research into terrorism and develops programs to counter violent extremism. The BSU, in addition to its own research, holds conferences and publishes books, newsletters, and practical guides for academics and practitioners.
Endnotes


2. Davis, Gareth and Steph Cockroft, ‘Europe’s jails are ‘breeding grounds’ for jihadists because ISIS see criminals as ideal recruits and one in five UK maximum security prisoners are already Muslim,’ *Daily Mail.com*, 12 October 2016. Available at: https://www.dailymail.co.uk/news/article-3833926/Europe-s-jails-breeding-grounds-jihadists-ISIS-criminals-ideal-recruits-one-five-UK-maximum-security-prisoners-Muslim.html/


6. Ibid. p. 7.


9. The Center for Mental Health Services, 1996.


14. Much of the text in this section is derived from materials developed by the New Zealand Department of Corrections, however, it is augmented following advice from other services.


17. The Centre for the Study of Radicalisation and Political Violence (ICSR), Kings College, London, UK.


22 One of the largest and most violent extremist Islamic movements in Egypt.

23 The second most important Egyptian Islamist Jihadi movement, whose former leader was Ayman al-Zawahiri, since 2011 leader of Al-Qaeda after Osama bin Laden was killed by US Special Forces.

24 Available at: https://islamonline.net/; 9 July 2007.

25 Munasaha [Advisory Committee] is also the name of the Saudi terrorist de-radicalization initiative, established in 2004.

26 The classification involves background check, psychological evaluation, analysis of education, skills, motivation and religiosity.

27 Recruiters are inmates who seek to radicalize other prisoners.


29 In 2001-02, more than 30 members of the Southeast Asian branch of Jemaah Islamiyah [Islamic Community] were arrested for plotting attacks on diplomatic missions in Singapore.


31 Training Institute, under the Ministry of Home Affairs, for the Singapore Police, Civil Defense Force, Central Narcotics Bureau, Prisons Service, Immigration and Checkpoints Authority and the Internal Security Department.
Bibliography


Davis, Gareth and Steph Cockroft, ‘Europe’s jails are ‘breeding grounds’ for jihadists because ISIS see criminals as ideal recruits and one in five UK maximum security prisoners are already Muslims,’ *Daily Mail Online*, 12 October 2016. Available at: https://www.dailymail.co.uk/news/article-3833926/Europe-s-jails-breeding-grounds-jihadists-ISIS-criminals-ideal-recruits-one-five-UK-maximum-security-prisoners-Muslim.html.


Web-based Resources

Confederation of European Probation (CEP)
https://www.cep-probation.org/knowledgebases/radicalisation/
Works with probation agencies in raising awareness of radicalization by organizing meetings and events

EUROPRIS - https://www.europris.org/
European organization of prison and correctional services. Provides information exchange, research, publications, workshops and expert groups

INTEGRA - http://www.integra-project.org/
Radicalization prevention approach for community corrections, probation and prison services.

International Corrections and Prisons Association (ICPA) - https://icpa.org/home/
International corrections association promoting professional and humane corrections. Has publications, working groups, training, research, and conferences.

R2Pris - http://www.r2pris.org/
Radicalization prevention in prisons. Site includes online training and radicalization risk assessment tools.

Radicalization Awareness Network (RAN)
European Union project. Website has videos, publications, references and links to useful organizations.

RAND Corporation National Security and Terrorism
Conducts, inter alia, research for U.S. Department of Defense and allied ministries of defense.

R4JUST – https://www.r4just.org/
Radicalization prevention competencies’ development program for justice professionals
Chapter 9

Prevention of Radicalization to Terrorism in Refugee Camps and Asylum Centers

Barbara H. Sude

Only a minority of refugees and asylum seekers become terrorists, but some have committed major attacks, raising concern among host country governments and publics. This chapter identifies factors that contributed to or deterred the rise of violent militant groups and terrorists among refugees confined to camps during major historical migration crises. It then examines current efforts to mitigate the same risks among today’s refugees in camp situations. However, more than half of refugees are not in camps, but are housed either among host country populations near the countries they fled from or in third countries, where many transition through asylum reception facilities before beginning to rebuild their lives. The main factors identified in the historical cases remain relevant to more recent situations: host government policies, security and radicalizer access, living conditions, opportunities for youth, and local economic conditions and resilience. Lessons drawn from programs by the United Nations and other stakeholders to address these factors also are relevant to third countries struggling to integrate refugees. As refugees become part of the wider society in new countries, other individual risk factors for radicalization to terrorism become key to prevention efforts. These factors are essentially the same as for non-refugees. Not all have been empirically validated, but to the extent that these are useful indicators, this chapter will examine how much they apply to refugees specifically and identify promising methods drawn from mental health, criminal justice, youth, and community programs to mitigate individuals’ susceptibility to radicalization before they commit violence.

Keywords: terrorism, counterterrorism, radicalization, extremism, refugees, asylum seekers, migration, prevention, mental health, education, crime, Europe, Middle East, Sub-Saharan Africa, South Asia, United Nations
The outflow since 2011 of more than five and a half million refugees fleeing conflict in Syria has made host countries increasingly apprehensive that these people, deprived of resources and traumatized by violence, will commit terrorist acts. Indeed, a small minority have, putting unprecedented pressure on governments to quickly identify radicalized individuals before releasing them into the community. A comparison drawn from academic research between historical refugee crises in which groups of refugees became radicalized and other crises in which they did not reveal sets of factors that appear to increase refugees’ susceptibility to radicalization. For example, large refugee groups in the past faced prolonged internment in camps, sometimes alongside armed militants who had contributed to the conflict. Camp conditions also presented daily survival challenges that in some cases added to refugees’ susceptibility to extremist recruitment. Although camps are no longer the norm for most refugees, many still face long periods of uncertainty in asylum reception centers or crowded urban accommodations with limited access to adequate housing, education, or employment.

What the historical comparison also shows is that many of these risks can be reduced with comprehensive policies from local, national, and international stakeholders to address long-term needs of refugee and host countries’ needs. The United Nations (UN) and partner non-governmental organizations (NGOs) worldwide already have made significant policy changes in that direction for current and future refugee groups. However, the decision to commit a terrorist attack is usually an individual one, and, as in past cases, some refugees may experience certain mental and environmental stresses that can make them targets for radicalization or even push them to violence. Social service, criminal justice, and psychology research suggests that intervention measures developed for non-refugee populations at high risk for violence may be applicable to refugees, and some are being tried in well-constructed programs. However, long-term studies are rare on which interventions or overall reforms of refugee systems will best deter individuals’ radicalization to terrorism and, even more importantly, their decisions to act.

Sourcing and Data Issues

This chapter, an expansion of the author’s exploratory study for the RAND Corporation (2015), draws from academic, governmental, non-governmental, and UN literature on historical and current migration, counterterrorism, mental health, and criminal justice issues relevant to refugee radicalization concerns, enhanced by interviews with a small group of specialists from several disciplines and media reports on terrorist incidents or host community concerns. The overall focus is on refugees and asylum seekers escaping Armed conflict or large-scale persecution across international borders, not economic migrants and people fleeing natural disasters not associated with a conflict. Internally-displaced persons (IDPs) or migrants will be discussed only where their status offers insight into comparable refugee situations. The specific subjects of discussion here are refugees housed in camps for the short or long-term, and refugees and asylum seekers sheltered in migrant reception centers, usually on a temporary basis. The latter discussion will also touch on short- or long-term settlement in the local host country community, the more common outcome for refugees today. This chapter will not attempt to provide a broad assessment of preventing or countering violent extremism (PCVE) measures, a subject addressed in greater depth elsewhere, except to raise attention to programs applicable to refugees. Border control issues also are addressed in another chapter.

In the historical case comparison for the RAND study, we broadly defined radicalization as “the process of committing to political or religious ideologies that espouse change through violence.” It includes enlistment in armed militant groups, such as irredentists or ethnic supremacists, that may or may not have been designated by governments or international organizations as terrorist groups at the time. Since the Al-Qaeda attacks on the US in 2001, governments, despite retaining terrorists of all stripes on global watchlists, generally have worried most that some Muslims inside their countries will adopt a jihadist ideology that
advocates violence as a religious duty. This concern, rightly or wrongly, dominates policy
debates about the risk of refugee radicalization today.

The literature we examined for the historical cases in the RAND study was quite broad in
terms of geographic area, time, and type of product. The authors generally benefited from the
ability to stand back from the events and weigh the credibility of a variety of sources, including
government records, media reports, and in-person accounts. In some cases, previous
quantitative studies existed. Drawing solid conclusions from the current refugee and asylum
center literature is more difficult. Almost all the data on refugee and asylum seeker
involvement in terrorism today is from Europe. Moreover, the data was analyzed soon after the
Syrian refugee crisis peaked between 2013 and 2016, when border posts and reception facilities
still were overwhelmed. Local authorities had to quickly recalculate how to cope with refugees
at the same time law enforcement was responding to major terrorist attacks, and those factors
may have influenced conclusions.

The issue that looms largest in any evaluation of either the risk of terrorism among refugees
and asylum seekers or the efficacy of prevention measures is the very small proportion of
refugees who resort to terrorism. Refugee specialists stress that violent extremism is more
likely to trigger migration than result from it. The oft-cited data analyzed by the Cato Institute,
a US libertarian think-tank, is illustrative of this: of the 3,391,203 refugees admitted to the US
from 1975 to the end of 2017, 25 were terrorists; of those only three were successful. Of the
732,168 asylum seekers admitted from 1975 to 2017 later emerged as terrorists, including the
2013 Boston Marathon bombers. As for Europe, Sam Mullins of the George C. Marshall
European Center for Security Studies notes that, although the data on total numbers of refugees
and asylum seekers are not definitive, official EU statistics count 4,558,005 first time
applications for asylum between 2011 and 2017. Mullins assesses that only 144 refugees or
asylum seekers who entered Europe during the period have been credibly accused or convicted
of involvement in terrorism.

Recommendations for prevention measures are dependent on identification of “risk
factors.” Governmental and academic sources provide lists drawn from known terrorism cases,
but empirical assessments of the validity of the factors are few. The motives for engagement
in terrorism between refugee and non-refugee individuals are very similar, as radicalization
studies show. The literature sometimes conflates criminal activity, or just a propensity for
violence, with a higher terrorism risk without fully documenting the specific conditions that
would make the connection valid for refugees. It also presents correlations between
numbers of refugees and numbers of terrorist incidents, both domestic and international, without
demonstrating causation. Assessments focused on Europe sometimes mix concern about
refugees with worries about the repatriation of European citizens trained by terrorist groups as
“foreign terrorist fighters.” Several programs to avert radicalization show promise for
addressing problems many refugees experience when they begin to integrate in a new
environment. However, evaluations of program outcomes over time still are sparse.

Radicalization of Refugees in Camps: The Historical Experience

Any discussion of refugee radicalization in camp settings would have to address key historical
cases in which camp-based refugee groups became militarized, conducted cross-border
operations, and sometimes radicalized enough to mount terrorist attacks well outside their
original regions. Examples that stand out are Palestinians in Lebanon after the creation of
Israel, Afghan refugees in Pakistan during and just after the Afghan-Soviet war, and Rwandans
in Zaire/Democratic Republic of Congo (DRC) after the Rwandan genocide. Such “worst
cases” contribute to impressions that refugees represent an inherent risk of violence, that they
naturally become “refugee warriors” for a cause. Not all refugee situations, even camp
situations seemingly similar to those cases, present the same risks, and only about 40 percent of refugees reside in camps in recent years.\textsuperscript{8}

A careful comparison of these cases with similar situations in which refugees did not radicalize reveals a set of common factors that appear to heighten the risk and perhaps could be mitigated in future such scenarios. In all of the cases, massive migration taxed the international relief community and the host country. The refugee camps were crowded, the refugees were suddenly impoverished, and often crime and violence, such as smuggling, rape, and murder occurred. However, one did not necessarily see organized armed groups or terrorists emerging.

For the RAND paper, we examined nine refugee cases in detail, supplemented by a less detailed examination of four additional ones.\textsuperscript{9} We initially selected 16 variables as potentially relevant to radicalization for both camp and non-camp settings. They included the refugees’ numbers; reason for fleeing; ethnic and religious differences; legal status; type of housing; employment and education; the presence of armed groups; and receiving and sending state policies. From our examination of the historical literature, plus interviews with experts, six groups of factors, somewhat overlapping, emerged as most relevant for understanding why radicalization emerged in the “worst cases” but not in the others, although establishing a hierarchy would require further study:

1. The host country’s administrative and legal policies, such as restrictions on refugee movement, registration, employment, and education.
2. Lack – or militant control of – security, particularly in and around camps.
3. Political and militant organizing among the refugees, sometimes with host country encouragement.
4. The type of shelter for refugees, notably isolated camps with poor living conditions and/or close proximity to the border of the country the refugees fled.
5. Conditions for refugee youth, including education and employment opportunities.
6. Local economic conditions and resilience within the host country, such as availability of public services or employment.\textsuperscript{10}

\textbf{Palestinians}

As of 1950, 750,000 Palestinians had fled their homes, most to neighboring Arab countries. Those states often exploited displaced Palestinians to gain advantage in the overall Arab-Israeli conflict and initially, at least, did not officially recognize them as refugees. The Palestinians themselves did not first seek to integrate into the host countries, hoping to return home. Many settled in camps, where a dedicated UN entity, the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA), became responsible for humanitarian efforts.\textsuperscript{11} The main factors of radicalization in this historical case appear to have been the political and militant organizing and lack of security in the UNRWA camps, partly attributable to host country policies – the host country, not UNRWA, being responsible for policing.\textsuperscript{12} Lebanon, Jordan, and Syria treated the refugees differently, with different results which are discussed below.

Lebanon restricted the refugees’ freedom of movement, employment, and education outside the camps and proved unable to provide security for the camps.\textsuperscript{13} As the number of refugees increased after Israel’s occupation of the West Bank in 1967, Beirut ceded control of the camps to the Palestine Liberation Organization (PLO). According to a University of London specialist who conducted research inside the camps, the militants offered important educational opportunities for youth alongside a liberation narrative that helped encourage attacks in Israel and globally.\textsuperscript{14} Even after PLO leaders were ousted in 1982, the camps remained trouble spots, where, in the 2000s, Islamist extremist groups vied for control.
Jordan, with the largest Palestinian refugee presence, gave the Palestinians citizenship, but King Hussein initially turned a blind eye to militant activity in camps and other Palestinian settlements, which became virtually self-governing states. Only after nearly succumbing to an attempt by armed Palestinian factions to overthrow the monarchy from the late 1960s to 1971, did Amman oust militant leaders and develop a strong internal security apparatus.

In Syria, which had intervened on the Palestinian side in Jordan, Hafiz al-Assad gained control by late 1970, also building a pervasive security apparatus. Damascus harbored Palestinian militants, such as the Popular Front for the Liberation of Palestine-General Command, for its own ends, giving the regime insight into militant activities, while the groups mounted terrorist attacks outside Syria. Both Jordan and Syria allowed Palestinian refugees to travel internally and work outside the camps, although Damascus did not grant them citizenship, and both countries generally avoided internal terrorism from Palestinian groups after the 1970s.15

Afghans

Some 6.5 million Afghans fled drought and the Soviet invasion just before and during the 1980s, mainly to Pakistan and Iran. About 6.2 million fled internal chaos in the early 1990s following the Soviet defeat. The differences in the level of radicalization between the 1980s and 1990s in Pakistan and between Afghans in Pakistan and those in Iran are significant and include both camp and non-camp situations. Host country policies on freedom of movement and political activity, in particular, shaped the differences. In the first wave, both countries were welcoming. Informal camps arose in Pakistan, which allowed the refugees freedom of movement and economic activity, including establishing a trucking industry there. Refugees in Iran generally resided outside camps, moving freely to find employment, with the government providing access to education and health services. When the outflow of refugees became overwhelming during the Soviet invasion and after, Iran mainly cut benefits, while Pakistan forced the refugees into camps close to the Afghan border, notably into the tribal areas where Islamabad had less control, and restricted the United Nations High Commissioner for Refugees (UNHCR) access.16 Islamabad also increasingly encouraged NGOs associated with the Islamist militant groups fighting the Soviets to register and educate the refugees and recruit them for the war. Access to aid — at a time international refugee funding was declining — became dependent on membership in one of the militant parties Pakistan supported.17 Those parties contributed to the chaos of the Afghan civil war in the 1990s and the rise of some extremist groups still active today and attracted support from foreign fighter groups like al-Qaeda.

Rwandans

The refugee crisis during a civil war in Rwanda developed quickly following the massacre in mid-1994 of more than 500,000 ethnic Tutsis and moderate Hutus by Hutu extremist militia and the subsequent takeover of the country by a Tutsi insurgent force. The UNHCR and other relief organizations were unable to separate the Hutu armed extremists and former Rwandan armed forces members from civilians among some one million refugees fleeing to Zaire, where the extremists already had prepared the ground for a state-in-exile. According to an academic study by Lischer, the relief community inadvertently allowed the militia members to distribute food to the refugees to gain support and supplied dual-use equipment to which extremists gained access. Extremists even dominated so-called “civilian” camps, using them for cross-border attacks.18 As in the Palestinian and Afghan cases, host country policies also contributed to militarization of the refugees. Uganda in the early 1990s had rejected resettling Tutsi
refugees and encouraged their insurgency. President Mobutu Sese Seko of Zaire supported the Hutus, but his successor, who renamed the country the DRC, opted to support the Tutsis. The Rwandan crisis grew into a series of armed conflicts throughout Africa’s Great Lakes region.

How Can Radicalization in Camps Be Prevented?

In all of these cases, refugees’ confinement in camps for long periods in itself played a direct role in their radicalization. The UNHCR in 2014 instituted a policy to better integrate camp refugees with the wider population around them, stressing that camps, albeit often necessary at the outset of a crisis, limit the rights of refugees “to move freely, choose where to live, work or open a business, cultivate land or access protection and service.” Refugees may be prohibited from working outside the camps and may become dependent on relief aid for their daily needs and on rumors as the source of information about their futures. Where armed militants control the flow of both aid and information (or warring factions dwell side-by-side) it is no wonder that some refugees fall prey to radicalizers. With or without militants exercising control, an International Crisis Group (ICG) study in Turkey found that young people face particular stresses, as “children born in camps are constantly exposed to stories of suffering, sorrow, bloodshed and loss that magnify the trauma of living in a closed environment.” Sexual abuse, even between children, can be “widespread.”

Budgets, however, often constrain access to psycho-social counseling. Conspicuous camps with apparent free-flowing handouts to refugees also can spark hostility toward the refugees within the host country population, increasing insecurity.

UNHCR’s 2014 policy envisioned increased cooperation with host country governments and local communities to address security concerns and open greater opportunities for refugees to rebuild their lives. Reliance on camps could not be eliminated as the Syrian crisis exploded after 2013, but UN agencies have been working with NGOs both to improve camp conditions (with a view to transforming those that must remain as ordinary settlements, and to build new resources in local communities to help decrease resentment and enable them to absorb refugees into schools and jobs. Many refugees have been settled among host-country populations, with less than a quarter of Syrian refugees in Jordan, for example, still in camps.

Preventing Radicalizer Control/Influence: Camp Administration

Some of the historical crises suggest that camp tensions, including domination by armed groups, can be alleviated when civilians in camps are given a greater say in their own governance, selecting leaders they can trust and giving them outlets for peaceful resolution of grievances. It helps when they see familiar institutions from home re-established, but doing that requires careful consideration. For example, in the 1990s, Somali and south Sudanese refugees in Kenya, who had fled brutal inter-clan and tribal warfare, transplanted court systems that, in the Somali case “sometimes reflected clan or gender biases” and in the Sudanese case, were too reliant on corporal punishment. The latter system, moreover, soon fell under the influence of Sudan People’s Liberation Army (SPLA) insurgents. By 2013, however, the huge Dadaab Somali refugee camp complex in Kenya was able to conduct elections that helped increase the representation of women and youth. Jordan set up Sharia courts in the Za’tari camp, partly to provide official documentation to families, in the first years of the Syrian crisis.
**Preventing Radicalizer Control/Influence: Security**

The historical cases demonstrate that improving security, whether by better host country policing around the camps, sometimes with foreign assistance, or by tighter control of resources and improved protection inside the camps, can deter militant influence. To undercut SPLA influence in Kakuma camp, the UNHCR, by 2000, helped train Kenyan police and set up a guard force in which locals worked with refugees, providing work for both.26 As the Syria crisis mounted in 2013 and 2014, camp administrators in Turkey greatly restricted access to camps, “to protect the refugees from the risk of provocation by outsiders visiting the camps and to preserve the dignity of the refugees,” according to a report by the Brookings Institution.27 Jordan established a police presence in the Za’tari camp. In the face of continuing crime, such as sexual exploitation and human trafficking, Turkey’s Migration Directorate in 2018 began offering able-bodied refugees rent money incentives to leave camps as part of a plan to leave only vulnerable people under camp protection.28 Refugees today, whether inside or outside camps, are usually registered with their biometric data such as iris scans, and given vouchers and debit cards. Some places even use iris scans in lieu of a card to shop for necessities.29 European countries such as Greece also have improved intelligence gathering through undercover work or informants inside refugee concentrations to help detect infiltrators, according to Mullin’s research.30

**Preventing Youth Recruitment**

Militants historically have sought to indoctrinate and potentially recruit youth in camp communities as evidenced in the cases of Palestinian and Afghan refugees. Interviews for the RAND study and academic literature on non-refugee radicalization stress that the factors influencing an individual’s risk differ little between refugees and non-refugees. Economic deprivation, for one, is not always relevant, but personal factors and peer influence usually are. Personal risk factors emerging from the literature on refugee youth (usually defined as between 15 and 24 years old) center on loss of access to opportunities for education, social entrée, and stable employment.

**Providing Education**

The Syria crisis prompted an international commitment to “No Lost Generation,” but tight aid budgets for refugee schools and host country restrictions on access to universities mean that education beyond the primary level is often lacking. In the 1990s, crime increased among Somali youth in Kenyan camps when secondary education was dropped, and decreased funding meant that militant Islamist groups assumed responsibility for educating Afghan youth in Pakistan.31 UNICEF, in 2014, found in interviews with a small group of Syrian refugee children in Jordan’s Za’tari camp that some wanted to join armed groups like the Free Syrian Army (FSA), partly because of boredom and lack of educational opportunities.32 More recently, with the assistance of foreign universities and several NGOs, college-level courses focused on teacher training, have been offered in the Dadaab camp complex in Northeast Kenya, which also has as many as seven secondary schools.33 Several foreign universities and Google cooperated to set up a connected learning hub in the Azraq camp in Jordan.34 Studies by the American University in Beirut produced recommendations to address obstacles to higher education for refugees in Lebanon, such as lost school documentation, noting that the Ministry of Education and Higher Education was taking tentative steps to resolve at least qualification issues.35
Mitigating Discrimination

A youth’s resentment of perceived social discrimination and injustice, worsened by gender-based and other forms of violence in and around the camps, can also increase susceptibility to radical pitches. A study in 2015 by the NGO Mercy Corps of non-refugee and refugee youth in three conflict states found that experience with injustice and discrimination, including perceived favoritism toward corrupt elites, was more important than poverty or lack of employment in their involvement in political violence. The NGO recommended coordinating “intercommunity peace building and governance reform” alongside jobs training and counseling in programs with a dedicated youth focus.36 Young Somali refugees in Yemen were more likely to be radicalized than Somalis in Kenyan camps because they faced discrimination in Yemeni schools, according to a study published by the Belfer Center.37 Indeed, part of the rationale for improving educational facilities in Dadaab was to avoid the discrimination refugees faced when they traveled outside the camp. The multi-agency “Amani” program begun in 2014 in Jordan for refugee and local communities’ aims to reduce discrimination, gender-based and other forms of violence, coercion, and discrimination. A program originator, the Child Protection Sub-Working Group, coordinates UNHCR, UNICEF, and youth-oriented NGOs there to improve education and counseling, reduce school bullying, and increase access to the justice system for refugees and non-refugees alike.38

Creating Work and Recreational Outlets

The search for employment is a constant problem for many refugee youths, but what work they can find is not often the type of activity that will build secure futures and offer meaningful social engagement or skirt militant influence. As families lose breadwinners, with some children having left on their own or becoming heads of households, child labor can become a default coping strategy in both camp and non-camp settings, keeping children out of school. Early in the Syria crisis, the Jordanian Ministry of Labor estimated that some 30,000 refugee children were working, some in risky or exploitative occupations.39 More recently, American University in Beirut (AUB) researchers found that young Syrian refugees offered college scholarships often felt compelled to work instead to support their families.40 In fact, there are often few counseling programs or meaningful activities for young refugee school dropouts or those over 18 that will help them integrate into new settings and build futures, according to an ICG report on Turkey, which recommends language and literacy courses, alongside enhanced sports and arts programs.41 Although some experts feel that activities like sports targeted at “keeping them off the streets” have little value, others see significant value.42 The Greek experience seems to support the latter. A local soccer club on the island of Lesbos began taking youth from local refugee camps, and in 2019, when Athens changed its laws to allow refugees and asylum-seekers to join national sports teams, an African migrant on the Lesbos team qualified for a Greek team, greatly boosting the morale of the refugees.43

A key component of opening up opportunities for refugee youth (and their elders) is allowing them to leave the camp environment at least part of the time and obtain work permits, something some host countries are still reluctant to do. In early 2019 Ethiopia, host to the second largest refugee population in Africa, passed a law allowing refugees previously confined in some 20 camps to move around to find work and attend school with Ethiopians. The move is part of the national program to stimulate job creation, with 30 percent allocated for refugees, in response to new UN-sponsored refugee policies.44
Preventing Host Community Hostility: Building Local Partnerships

It is indisputable that an influx of thousands of refugees into an area where resources already are scarce can trigger resentment and even violence. Host community engagement, then, is critical for creating viable jobs for everyone and lessening refugees’ impact on schools, public and social services, and natural resources. This is central to the UN’s Global Compact on Refugees, signed in December 2018, as well as the earlier Regional Refugee and Resilience Plan (3RP) for the Syria crisis and the Alternatives to Camps strategy. In 2012, when locals in Kenya blocked roads to refugee camps demanding jobs, the NGO CARE began plans to build up banking in the area and lessen the camps’ impact on the environment. Refugee organizations more recently worked with local businesses to better target vocational training – providing training, internships, and work placement to locals as well as refugees. They repaired schools in Egypt and Turkey and refurbished housing – providing rent subsidies to locals and refugees – and water and sanitation facilities in Jordan. In Lebanon, UNICEF is working with NGOs to give unemployed refugee and non-refugee youth digital skills and foster entrepreneurship, while the International Labor Organization (ILO) is helping integrate Syrian workers into Turkish workplaces. There are emerging efforts, also in Turkey, to better utilize the skills of Syrian refugees who arrived with higher education and experience as teachers, healthcare professionals, or as technical specialists, who could establish businesses. In 2018, the UN and partner NGOs placed 3,500 Turkish and Syrian people in jobs and supported 1,200 to start businesses. In Bangladesh, where a renewed influx in 2018 of Rohingya refugees from Myanmar was overwhelming host populations, UNHCR’s Joint Response Plan envisioned hiring local businesses as much as possible to supply food and other needs to refugee camps rather than relying on handouts of large shipments from outside.

Obstacles to Prevention Efforts

As in the historical cases, host country actions and inactions still complicate or even block measures to prevent radicalization. Security lapses remain a major pitfall. During the Syria crisis, some host countries backed combatants in the civil war, contributing to militarization of refugee groups. Terrorists also likely gained at least a temporary foothold in camps in some cases, although the reports are mainly anecdotal. Some attempts at reforming camp administration have fallen flat and funding for measures most likely to deter radicalization continues to fall short. Greater freedom of movement for refugees, including closing camps – however important for refugee futures – naturally will further complicate policing, but, as noted above, camps can be closed societies in which crime and abuse can flourish.

Extremist Recruitment

Sometimes countries failed to note terrorist recruitment. Turkey and Jordan initially supported, turned a blind eye to, or failed to control anti-Assad insurgents. Ankara, as recommended, separated Syrian anti-regime fighters from the general population in separate camps, but because Ankara sympathized with the insurgency and was facing such a large influx, it was unable to prevent recruitment of refugees by radical Islamist groups like the al-Qaeda-related Jabhat al-Nusra (JN) and the Islamic State in Iraq and Syria (ISIS). As recently as 2018, interviewees told the ICG that, although Turkey was trying to stop ISIS activity, it was doing little against JN’s successor Hay’at Tahrir al-Sham (HTS). Jordan, too, separated some FSA combatants but allegedly ignored recruitment efforts among civilians, including recruiters with loudspeakers openly walking through Za’tari Camp. The counter-radicalization think tank Quilliam, in a report about youth recruitment, maintains that ISIS paid as much as $2,000 (US) in costs for enlisting a refugee in Jordan and Lebanon. Indeed, Jordanian special forces in 2016
reportedly found an ISIS “sleeper cell” in a refugee camp near Irbid. Authorities in Germany say a member of ISIS’ intelligence unit arrested there in 2017 had previously been tasked with recruiting in refugee camps in Greece. In 2018, ISIS members fleeing the collapse of their territory in Syria began appearing as ordinary refugees in Greece’s Moria Camp, sparking clashes with Yazidis whom ISIS had persecuted, and only belatedly coming to the attention of Greek authorities, who began to move Yazidis to smaller facilities.

Bias and Corruption
Local host country prejudice and corruption has proved difficult to eliminate, increasing refugees’ trauma and discontent and stymieing counter-radicalization measures. Following a terrorist attack by the Somali-based al-Shabaab group on Garissa University College in 2015, Kenya, long suspicious of Somali refugee involvement in terrorism, sealed off the Dadaab Camp, preventing refugees from leaving for school or jobs. The perpetrators proved to be Kenyan and Tanzanian, not refugees. Dadaab residents also claim daily humiliation due to local corruption and bias, such as having to pay bribes to get “free” identity cards or to get guards to recognize personal documents, and say they face harassment for reporting crimes.

A commentary by academics in Jordan saw an increase in open individual corruption by civil servants and high-ranking officials there since the Syrian crisis began, despite an anti-corruption campaign by King Abdullah.

In Turkey, border officials remain susceptible to bribes from smugglers, although Ankara has taken steps to improve security.

Funding and Reform Shortcomings
Historically, funding for crises has fallen off after the first few years. Although planning for Syrian refugees is much better than past situations, many of the aid budget line items most critical to preventing radicalization are underfunded. In particular, in the 2018 annual report for the “3RP” plan for the Syrian crisis, “livelihoods and social cohesion” – the core of creating jobs in cooperation with host countries – was funded at only 17 percent in Lebanon and “resilience” (supporting education and health personnel and helping municipalities) at 37 percent overall. Female-headed households still have problems accessing employment in several countries and unaccompanied children remain at particular risk for meeting even basic needs. School attendance still lags in some countries. Protection programs, including psycho-social services for children, were underfunded significantly in Iraq as of mid-2019. Even though refugees are playing a greater role in camp administration, the effort bears closer scrutiny and follow-up. In early 2016, Foreign Policy reported that refugees in Kenya’s Dadaab camp complex felt they had no real control over their situation despite elections.

Camp Closure and Repatriation
International community efforts to eliminate camps have focused on first, housing refugees among the population in the host country (or a third country), or second, allowing them to return home if it is safe to do so. The first option is covered in the second part of this chapter. The second option) has been a serious consideration in a few current cases. Some Syrians have gone home as the regime has begun to regain control, although the percentage of Syrians returning remains very small as of mid-2019, with only two percent returning when the border with Jordan reopened. Kenya has long wanted to close the Dadaab complex and has intermittently pressured refugees to leave. Although the international community has lately worked with Nairobi to prevent forced returns, continued insecurity and poverty in Somalia
has put those who have decided to go home at risk of radicalization. The Quilliam foundation found, for example, that al-Shabaab recruited former refugees by offering them needed aid.61

**How Much Do Asylum Reception Centers Contribute to Radicalization Risk?**

In the face of large-scale migration, reception centers for refugees and asylum seekers serve much the same function as camps and share some, but not all, risks. They provide refugees with basic necessities of life, including shelter, while the refugees await decisions on their future status, such as temporary or permanent resettlement in the host or a third country. Unlike those in border camps, refugees in asylum centers lack the option of immediately returning home, unless deported by host authorities. In fact, they may already have decided against returning, having deliberately traveled to seek resettlement. While refugee camps may persist for decades and become cities, asylum centers are designed for a short-term transition.

Although most asylum facilities are farther from the spillover violence of a war front, other radicalization factors may remain including:

- host country government policies, such as employment restrictions;
- poor living conditions, with restricted access to information;
- radicalizer access to the refugees;
- lack of security, including exposure to intercommunal violence;
- lack of opportunities for youth; and
- difficult local economic conditions.

The level of radicalization risk differs across the various phases of the asylum process, from initial reception to full integration into the host community. The experiences of high and middle-income countries, such as European Union (EU) countries, Turkey, Jordan, and Lebanon, highlight particular risks in the transition from the refugee aid safety-net of a camp or asylum center to integration. The process of integration can intensify the influence of the factors above, but each phase carries some risk.

**The Reception and Asylum Center Phase**

In the EU, conditions for asylum seekers differ from country to country, despite attempts at standardization. Under the “Dublin Regulation” of 2003, as revised in 2013, member states are expected to follow some common standards, with the country of entry usually responsible for asylum applications, although responsibility can be transferred via a complex set of rules. Asylum seekers have the right to a personal interview and can appeal transfers to another EU country to ensure they get a fair hearing. Transferring unaccompanied children and detaining asylum seekers are last resort measures. The administrative phase for asylum claims is supposed to be about six months.62 Reception centers, as of 2013, were to provide a basic standard of living, counseling when needed, and protection for vulnerable people or those with special needs. They would allow access to the labor market within nine months. Additional, more specific guidance on standards for reception facilities, much of which the EU had already tried to apply as of 2019, was drafted in 2016.63

**Living Conditions and Bureaucracy**

Asylum seeker housing varies across the EU and consists of either dedicated centers or a variety of facilities, including hotels and private homes, although some countries just provide a housing allowance. The type of facility often depends on the phase of the asylum process:
for example, transit centers or initial reception centers in the first stage, the latter sometimes essentially a camp. It is not uncommon for a country to spread asylum seekers around to avoid segregating them in one area.

Whatever the ideal situation might be, asylum seekers in some countries live with uncertainty and frustration about their status for more than a year, sometimes in accommodations that are far from recommended standards. In the UK before 2011, children were often placed in immigration detention facilities with their families for long periods of time; small numbers were still there as of late 2018. Spain received 47,810 applications for asylum between 2010 and 2016 but resolved only 41 percent of those cases during that period, although the law mandates a three to six-month decision period. The large influx of Syrian refugees in 2015 was only one factor - Sub-Saharan Africans as of 2018 also faced major delays. According to researchers who interviewed 1,000 refugees in the Netherlands, in 2013, many asylum applicants were assigned to rural areas far from jobs and schools, and the average stay was 21 months. Facilities also lacked privacy and schedules for personal activities or practice with the host language. Elsewhere, people have too little to occupy their time. “People that come here are dying of boredom… We have people that have been here for a year, eighteen months, that have nothing to do but look at the internet,” according to an asylum facility staff member Mullins interviewed. They may feel completely detached from the host country: a Syrian refugee in Ireland told a researcher that people in his Direct Provision center felt “really isolated,” with few, if any, outside contacts.

Radicalizer Access and General Security

Even if refugees and asylum seekers have been carefully selected for placement in a dedicated reception facility, authorities occasionally miss radicalized individuals. They may accept people to a facility, unaware they were already radicalized in the country or en route to the country, or had arrived as intentional terrorist infiltrators. Facility managers also may fail to prevent local radicalizers’ gaining access to the residents. As the Syria crisis mounted, European authorities were said to have lost track of many refugees, who then blended into the population. They also had a difficult time vetting asylum seekers who lacked identity documents or had deliberately destroyed them for a variety of reasons, often just to conceal personal factors that would preclude asylum. Anis Amri, a Tunisian who attacked the Berlin Christmas Market in 2016, concealed his petty criminal history. He pretended to be a minor and was housed initially in a youth asylum facility. Later radicalized in jail, he moved around Europe under various identities staying in asylum facilities. Immigration personnel missed some operatives from ISIS and other groups deliberately smuggled among the refugees, such as in the case of some of the November 2015 Paris attackers.

Outside, radicalizers also can gain access to asylum accommodations if visitors and newcomers are not checked carefully or staff do not report unusual activity. In 2015, when asked about “Islamic extremists using refugee reception centers as recruiting grounds,” the Director of Norway’s Police Security Service told Dagbladet newspaper, “It’s a scenario we are aware of.” Two Moroccan-national ISIS recruiters falsely claimed asylum in Portugal and brought over other asylum seekers, using access to asylum facilities there to indoctrinate them. The two became part of a continent-wide terrorist network, disrupted in 2016, planning attacks in Paris. In Italy the same year, a young Somali imam, who preached sermons praising ISIS, al-Qaeda, and al-Shabaab, tried to recruit the residents of a refugee reception center to attack a train station. The residents turned him in to the police. Refugees in identifiable asylum facilities face other threats that add stress and may increase susceptibility to radicalization. Anti-immigrant sentiment is increasing in many countries, and Muslim immigrants are often singled out. Facilities throughout Europe have been attacked by anti-refugee individuals and gangs, including fire-bombings, stabbings, and bludgeoning.”
2015 alone, Germany recorded 900 incidents and Sweden recorded 50 incidents. Anti-refugee activism is also pressing some countries to enact more restrictive laws that decrease options for refugees and asylum seekers.

**Moving into the Host Community: The Integration Process**

The integration stage, social scientists stress, is a gradual process in which refugees must renew or replace resources they have lost to begin to build a new future. These resources are more than material ones and include social and cultural relationships; status; and self-worth. According to migration specialists, a refugee also starts at an inherently unequal power position compared to the host society in multiple dimensions: economic, political, social, and cultural as well as individual, group, and community. Lengthy stays in asylum centers can either help the rebuilding process by providing language training and good local orientation, or hinder it by postponing orientation to avoid raising asylum seekers’ hopes and restricting interaction with locals.

After what may or may not be a short stay in a camp, reception, or asylum facility, refugees are expected to reside in a variety of housing arrangements in the host community, acquire jobs or attend school. In Turkey and the Middle East, the UNHCR and NGOs usually are still responsible, in cooperation with the host country, for the settlement of refugees in communities in lieu of camps as discussed above. In Europe, the practice is generally to transition those approved for asylum into life in the new country, with assistance and counseling in the beginning. The status of those rejected for asylum and not deported, but no longer entitled to services, remains a troublesome question in some countries, especially when the country of a refugee’s origin is unwilling to cooperate.

**Housing**

Refugees often have difficulty finding satisfactory housing, whether assisted by a refugee agency or on their own, because of financial or bureaucratic obstacles, social requirements, availability, or anti-immigrant bias. Some governments, such as Spain, have tried to avoid concentrating refugees in one city or neighborhood, partly out of fear that enclaves interfere with integration and may increase the risk of both exposure to radicalizers and anti-immigrant attacks. Immigration specialists there found in interviews conducted between 2016 and 2017, however, that refugees sometimes seek family or other people from home and move out of assigned areas, with or without authorization. If refugees do try to integrate, they often find that landlords will not rent to them. In many locations, refugees must share housing because rents are too high, as in parts of Turkey, or the accommodation they find is in slum areas. Syrian refugees in Jordan had to resort to poor housing as they exhausted the money they had brought with them. The Netherlands grants some asylum seekers a five-year temporary residence status, but permanent status, which requires command of the Dutch language, is needed to get mortgages and other services.

**Employment**

Finding a job is arguably the most challenging hurdle in the integration process for adults. Refugees who held professional positions in the home country are likely to find themselves in jobs with greatly reduced status, or unemployed. Some governments have raised barriers to employment: in Lebanon, Syrians are restricted to agriculture, construction, and environmental jobs, while Ireland, until 2018, banned asylum-seekers from working. Even where they are free to work, refugees may run out of initial financial assistance – 18 months in Spain, for example
– before they have secured a stable job, especially where the local economy is in a recession. A Syrian refugee told a Spanish interviewer that although assistance was ending, “neither of us have work, neither my husband nor me…we don’t know what will happen….we’re looking for work, but haven’t found any.” In Germany in early 2018, 80 percent of refugees were unemployed. Refugees may have lost documents showing their professional certifications or be required by local boards to take additional training that can be hard to access. Turkey as of 2016 granted Syrians under Temporary Protection Status the right to work permits, with the caveat that they are not to work outside the province where they were assigned. Many have moved to find work, however, and legal uncertainty is one factor discouraging employers from hiring them, particularly for higher-skill jobs. Refugee doctors and teachers may serve only Syrians.

Youth Education and Integration

Refugee children, seemingly in a better position than adults to absorb new languages and assimilate into unfamiliar cultures, still face multiple obstacles. Where local governments, refugee agencies, and communities are unable to provide essential needs, radicalizers may step in. European Asylum Support Office (EASO) guidance recommends that children get access to education as soon as possible in the reception process so that they can begin social interactions, but there can be long waiting periods, lack of trauma support and tailored curricula, and long distances to go to attend school. In addition, some older children may have missed schooling, while those above compulsory school age may not qualify for secondary school, but be unable to access vocational training. In Turkey in 2013, only 10 percent of urban refugees had access to education, for which they required a passport, police registration, and a residence permit, according to a Brookings report. As late as 2018, the ICG found that unspecified “large numbers” of teenage Syrians, who often struggle with Turkish, were not in school, in part because Ankara had ruled that only government institutions could provide education in closed special temporary Arabic-language educational centers in 2017. Few youths there received support for trauma.

Discrimination inside and outside the classroom imposes additional stress. Syrian refugees in Turkey complain of teachers who assume they are “ill-behaved,” intensifying classmates’ biases and bullying, according to the ICG. A migrant parent in Seville, Spain, told researchers that her children rarely experienced classroom bullying, but other interviewees in Spain complained of daily slights on public transportation and elsewhere in the community – forms of discrimination youth undoubtedly feel as well. A study of first and second-generation immigrant youth in Barcelona found that social exclusion increased in-group loyalty and contributed directly to the type of rigid thinking or “sacralization of values” that can be signs of incipient extremism.

Where Radicalizers Move in

At any stage in the integration process, radicalizers may try to step in to fill gaps in aid provision or otherwise try to influence the refugees. We saw that in some cases, radicalizers tried to enlist refugees in border camps directly into armed groups. In urban areas in the Middle East or Western countries, they may try to fulfill, for example, educational, religious, or even recreational needs to recruit refugees for terrorism. One motive for Ankara’s requirement that the state provides education was to bypass extremist proselytizing, but ICG researchers found some civil society groups were offering Arabic-language religion and morals courses as well as athletics. Unregistered, the courses either escaped review by Turkey’s religion directorate or were checked by inspectors lacking Arabic skills. The groups were not necessarily extremist,
but some courses concealed jihadist ideology. Amri, the Tunisian attacker on the Christmas market in Berlin, took classes at a Qur’an school in Dortmund, Germany, run by an alleged senior deputy to the head of ISIS’ recruitment network in Germany. In Spain, a Moroccan-born extremist allegedly offered boxing lessons to recruit disadvantaged Muslim youth to ISIS; he had ties to one-time boxing student Yahya Nouri, a co-conspirator in the disrupted 2016 ISIS plot to attack Paris.

Detecting and Preventing Radicalization

Given several devastating attacks linked to asylum seekers in the past decade, governments face unprecedented public pressure to identify radicalized or at-risk individuals before releasing them into the community. Indeed, once refugees become part of the wider society, determining whether they are becoming radicalized is more difficult than in a camp or asylum facility where aid organizations and law enforcement may witness their actions. Counterterrorism specialists have developed, based on studies of known terrorists, lists of indicators, symptoms, and risk factors that an individual – refugee or non-refugee – may be embracing a violent extremist ideology or readying an attack. The question is whether refugees are more or less likely to exhibit those characteristics, even if only a small minority of them commit acts of terrorism. If a refugee does show such signs, when should the authorities be called in? When is it ethical for an asylum center staff member or aid worker to report a person in their charge? Will casting unwarranted suspicion in itself increase the risk that the person will be alienated and radicalized? What existing programs show promise for mitigating personal risk factors or defusing radicalization in the refugee context?

In a 2019 handbook on indicators of mobilization for attacks, the US National Counterterrorism Center (NCTC) lists four general long-term “risk factors” for terrorism, essentially personal behavioral issues, that invite consideration in the refugee context: inability to cope with changes or perceived failures in relationships, school, or career; a history of personal use of violence and unstable mental state; social isolation; and possession of, or familiarity with, weapons or explosives.

1. **Coping with change and failure**: Clearly, refugees have experienced significant upheaval in their lives and additional stresses in adapting to a new country, but many, having survived earlier challenges, are better able to adapt to new conditions. Perceived failure, such as the underemployment noted above, is another matter. Some psychologists have underscored personal “significance loss” as a key driver of radicalization.

2. **History of violence, mental state**: A personal history of using violence is rarer among those fleeing violence, although not unknown. However, studies show that the trauma and abuse that many refugees suffer can increase the radicalization risk. Serious mental illness is rare, however, even among refugees and, although post-traumatic stress disorder (PTSD) can be more common than in non-refugee populations, the prevalence is still small and usually confined to certain population groups, like those who experienced torture or prolonged detention or are unaccompanied and orphaned minors.

3. **Social isolation**: This term refers to any individual deliberately withdrawing from his/her social network – not “social exclusion” caused by others – and has not been flagged as a risk specific to refugees. A possibly related concern in the refugee context is alienation in the form of what has been called a “culture and identity crisis.” A preliminary study in late 2015 of first and second-generation Muslim immigrants in the US found that those who rejected both their own and the host culture, and faced
discrimination, suffered loss of significance and were more likely to radicalize than other immigrants.\textsuperscript{98}

4. **Familiarity with weapons:** As mentioned in the camp context, former soldiers or others with military experience may become part of the refugee mix if they are not filtered out. Particularly salient in this context in recent years are former child soldiers and indoctrinated youth freed from ISIS-controlled territory. A Kurdish-German trauma specialist in Iraq working with ISIS children in 2017 told an interviewer he is optimistic that such children can be rehabilitated, adding that previous studies have shown that at least half of people who have suffered similar trauma will not require clinical intervention.\textsuperscript{99}

**Identifying Radicalization**

Symptoms of radicalization can be hard to identify before an individual commits a violent act. Moreover, few of what the European Radicalisation Awareness Network (RAN) terms the “kaleidoscope” of social, political, and environmental factors contributing to radicalization – underemployment, limited education – have been empirically proven and, in any case, may not apply to a given individual.\textsuperscript{100} The staff of refugee and asylum facilities in host communities nonetheless are often expected to spot potential radicalization among individuals in their charge. In some countries, personnel are also asked to report suspicious individuals to local or national authorities. Staff struggle with the professional ethics of unfairly stigmatizing a person, worrying, for example, whether the report will become a permanent record even if suspicions were wrong. The guidance, such as noting people who stop drinking alcohol, work out heavily, or become more religious, can be ambiguous. Moreover, many specialists assess that overemphasizing religious expression in particular can actually contribute to radicalization.\textsuperscript{101}

As the numbers of refugees and asylum seekers grew, EU countries began to try to refine their guidance to refugee assistance staff, including offering additional specialized training programs, although the tension between law enforcement and refugee protection needs remains. In Germany, intelligence officers and police give asylum staff training on signs of extremism and how to distinguish what is of less concern. The effort helped staff at one facility flag an unaccompanied minor planning a mass killing.\textsuperscript{102} Denmark encourages broad collaboration among law enforcement and security agencies and a range of social, education, and health service organizations. A successful program for staff working with unaccompanied minors by the Danish Centre for Prevention of Extremism (PET) stresses the life skills and “motivational interviewing” methods used by PET. A RAN review of training programs in 2018 recommends training tailored to each asylum center staff, with the focus on safeguarding the individual, avoiding stigma, and partnering with refugees themselves. In Belgium, such training improved the quality of reporting, and reduced the quantity of less-useful observations.\textsuperscript{103}

**Prevention Measures**

Those who work with refugees and asylum seekers in Western countries sometimes utilize a variety of methods and programs developed in the last decade to address radicalization risk factors for both individuals struggling with trauma or mental issues, and groups such as youth trying to integrate in new societies. Additional programs are being developed, some of which strive to offer budget-sensitive interventions that non-specialists can implement. Beyond the individual, some community programs hope to modify or eliminate social exclusion and discrimination.
**Mental Health Interventions**

Even though severe mental illness is rare among refugees, practitioners have underscored the need for some level of psycho-social assessment and support, particularly for youth or anyone who has suffered abuse or traumatic loss. Expensive individual therapy often can be avoided except for cases of severe mental illness. Treatments may rely on counseling and cognitive behavioral therapy (CBT) administered by non-psychologists to mitigate trauma’s potential to spur dangerous behavior. Some promising new interventions focus on the overall social environment. Psychiatrists have developed a model called Adaptation and Development After Persecution and Trauma (ADAPT) to help mental health personnel tailor interventions. It posits five psychological pillars of mental equilibrium that refugees may have lost: “systems of safety and security, interpersonal bonds and networks, justice, roles and identities, and existential meaning and coherence.” A combination of “traumatic loss” and “extreme injustice,” for example, may eventually trigger an outpouring of “complicated grief and explosive anger.” The ADAPT model helped in treating PTSD in Iraqi refugees in Syria.104 Researchers from the RAND Corporation, the University of California at Los Angeles (UCLA), and the Los Angeles Unified School District (LAUSD) developed a trauma intervention program for school children that may be applicable to refugee youth. Cognitive Behavioral Intervention for Trauma in Schools (CBITS) tries to reduce symptoms of PTSD, depression, and behavioral problems to improve overall functioning and coping skills. Although designed for mental health professionals, the method has been adapted for use by teachers and school counselors.105 Mental health also is central to a specialized intervention program by the Netherlands National Support Center for Extremism focusing on immigrants who may have lived in ISIS territory and show signs of radicalization. Two experts, including one on mental health, assess each case and work with local center staff to implement an intervention plan over four “domains”: shelter and family; security; care; and education and work.106

**Criminal Justice Desistance Methods**

Criminal justice research and experience offer examples of promising intervention measures developed for at-risk, non-refugee populations to avert dangerous behavior. Some factors contributing to, or associated with, criminal behavior and recidivism are close to the risk factors associated with radicalization – to the extent that those factors are valid – and may be modifiable with similar methods.107 In the criminal context, they include antisocial thought patterns (including unwarranted justification and rationalization), anti-social associates, poor family ties or being unmarried, unstable employment, few leisure activities, and substance abuse. The idea in the criminal desistance field is to first address “dynamic factors” (those that can change over time), such as changing the people a person associates with and providing meaningful work and leisure. One study found that marriage was a significant deterrent to crime among immigrants. The city of Malmö, Sweden, has examined how criminal gangs provide strong social networks as a means to alter the pattern for refugees at risk of extremism. For factors more difficult to address, including thought patterns, specialists often turn to CBT. They also try to change mental patterns by gradually easing restrictions on the person, including jail time, as risk factors improve, a process called “Risk-Needs-Response.”108

**Youth and Community Programs**

Several European programs are attempting to avert radicalization among refugee youth by addressing risk factors such as social bonds. Some also work across the wider community of non-refugee youth to reduce social exclusion by changing entrenched viewpoints. The German
NGO Ufuq (“horizon” in Arabic) receives federal funding for projects on education and youth that try to deter refugee youth from radicalization through encouraging them to join social organizations and strengthen their personal skills. Ufuq also provides civic education for both refugee youth and their native-born peers to change extremist narratives and reduce prejudice and racism. Other European programs try to reduce extremist thinking in both communities by highlighting alternative views and the complexities in social issues. For example, the RAN polarization prevention model recommends a method in which mediators, rather than trying to bring opposite viewpoints together, first focus on the middle group as the target and change the subject to a question about the middle viewpoint. The EU Erasmus program focuses on marginalized youth and seeks to foster diversity. Its UK program guide for youth workers offers a variety of methods to loosen thinking, including sets of scenarios from different viewpoints. For example:

“When I walk in my neighbourhood, I notice these foreign students standing in street corners speaking in their own language. I feel unsafe.

[or]

Local youth workers in my neighbourhood are forming football teams and I notice that some of these people who are hanging about in street corners are great players. They really want to win the football tournaments just like I do and make our neighbourhood feel proud of us. I feel that we are more similar than I thought.”

Unintended Consequences in Prevention Methods

Governments are showing increasing interest in evaluating violent extremism prevention programs, but studies so far are few. Feedback from participants in asylum center staff training or recipients of handbooks on refugee screening has been scant. Some smaller scale studies have nonetheless uncovered possible errors in early assumptions about risk factors and pitfalls in some radicalization prevention methods often used in the refugee context.

- **Mental Health**: A study evaluating resilience training in the Netherlands aimed at increasing self-esteem, empathy, and perspective-taking skills (ability to anticipate the reactions of other people) among Muslim adolescents with dual identity found that, although empathy increased, self-esteem also increased narcissism in some subjects, a factor in susceptibility to radicalization. The study also found that perspective taking could increase negative feelings about non-Muslims and positive attitudes toward violence.

- **Desistance Efforts**: PREVENT, a program in the UK since 2003 to educate communities on radicalization risks and deter violence through preemptive interventions, has had some success in diverting people from extremism, but also has received significant public criticism as being discriminatory and possibly contributing to radicalization. Strengthening family and other social ties also can backfire. Studies of both Yemenis and West Bank Palestinians on factors deterring radicalization show that close friends and family can make a person more likely to approve of violence in theory (although not necessarily to engage in it personally), and that family play a greater role than friends. Studies also show that traditional community leaders tapped as potential role models can lose influence among fellow refugees far from home.

- **Civic Education and Engagement**: Refugee specialists recognize that refugees, like non-refugees, need an outlet for peaceful political expression, even in camp settings, and that political activism should not automatically be taken as a sign of radicalization. Nonetheless, political violence for some people is just one expression of legitimate political activism that they can rationalize. The NGO Mercy Corps has found that,
although the effect of civic training on youth can be neutral, training that sensitizes them to authorities’ injustice can make them more likely to radicalize. In host countries, anti-refugee assaults can have a similar impact.

**Conclusion**

Refugees face a host of challenges, having lost their homes and communities, their material resources, and sometimes even their sense of self-worth. Those left in camps are in limbo, unable to start new lives, and dependent on humanitarian aid. Others settled among host country populations may find their new homes far from welcoming, with suspicious, even hostile, neighbors and legal systems that make education and jobs hard to obtain. At each stage, radicalizers may try to gain the refugees’ trust, persuade them of the virtues of extremist ideologies, and even recruit them for terrorist attacks. Nonetheless, very few refugees become radicalized and even fewer commit acts of violence.

In the historical “worst cases,” large groups of refugees, even entire camps, became radicalized. Today the main concern is an individual refugee’s risk – essentially the same as for the rest of society. Although we have less understanding of why people do not radicalize than why they do, the message from many host country governments is that tighter security is the answer: no single terrorist refugee should be permitted to slip in. For that to happen, one would need to know how to identify a terrorist in the making long before he/she shows any signs, but the science is not developed enough for that. Alternatively, one could use the common risk factors thought to increase susceptibility to radicalization, as addressed above. Those factors still are too general, however, to identify in advance of any terrorist actions specific individuals at high enough risk to legally justify excluding them.

What host governments and the international community can do is to try to modify certain factors to mitigate any push toward radicalization they may create. Where camps are necessary this would mean giving refugees more control over their own lives, offering psycho-social support, providing post-primary education for young people, and building employment skills useful beyond the camp environment. Security measures will still be needed to protect refugees from abuse and discourage exposure to militants and radicalizers. Host communities must be supported in order to reduce hostility. When refugees leave camps for host societies or transition through reception and asylum facilities, they begin to take more personal control, but they also continue to need close, personally-tailored support to integrate successfully, whether by learning the local language and bureaucracy or rebuilding educational and job credentials. Some refugees continue to need mental health resources. Again, building host community receptivity – including countering anti-refugee extremism – is vital. Security measures in this phase must not only prevent radicalizer access to a refugee facility but also aid individuals there struggling with personal issues that might make them vulnerable to radicalization. That includes helping them develop positive personal associations.

The UN, organizations which support refugees, and many host governments already have taken steps to address risk factors that contributed to radicalization in past crises. Although their effectiveness over the long term has yet to be proven, the most promising programs benefit from coordination across agencies and fields of specialization, including careful cooperation between terrorism specialists in law enforcement and security services, refugee experts, and health professionals. They also consult the refugees themselves. Where costs are high, such as for individual mental health counseling, specialists are developing methods non-experts can apply. Nonetheless, the numbers of refugees have overwhelmed relief budgets, and full funding is probably impossible. What can be done is to give greater attention to programs that are seriously underfunded but directly address radicalization risks, such as livelihoods and community resilience initiatives or meaningful activities for youth.
Where programs fall short and societal biases prevent refugees from integrating successfully, studies have shown that their children may be even more likely to radicalize. Second-generation immigrants have conducted major terrorist attacks or volunteered abroad as foreign fighters. In Spain, where social exclusion of refugees is considered high in some areas, about half of 178 people arrested between 2013 and 2016 for terrorism-related offenses were second generation immigrants.\(^\text{119}\) Now that the major migration waves from the Middle East have eased, host country governments – and their citizens – must continue to foster policy changes that will ensure not only that today’s refugees can successfully create new lives but also that in the inevitable future crises those polices will discourage, not contribute to, terrorism.

Dr. Barbara Sude has served more than 30 years with the U.S. Government, where she specialized in analysis of terrorism, political Islam, Sub-Saharan Africa, and the Middle East. As an adjunct researcher and former senior political scientist at the RAND Corporation, Barbara Sude most recently focused on counterterrorism, refugees, and asymmetric warfare. She has given several public presentations and media interviews on counterterrorism issues and is the lead author of “Lessening the Risk of Refugee Radicalization: Lessons for the Middle East from Past Crises” (RAND Corporation, 2015) and co-author of “Knowing the Enemy: Understanding the Islamic State and Principles for Defeating It” (RAND 2017) and “An Economic Analysis of the Financial Records of al-Qa’ida in Iraq” (RAND Corporation, 2010). She received her BS in Arabic from Georgetown University and her Ph.D. in Near Eastern Studies from Princeton University.
Endnotes

2 Ibid.
9 Two cases of Rohingya Muslim refugees in Bangladesh (1975 to 1978 and 1989 to 1992); two cases of Afghan refugees in Pakistan and Iran (1978 to 1988 and the 1990s); Somali refugees in Kenya (1990s to 2000s); Rwandan refugees in Zaire/DRC (1990s-2000s); Palestinian refugees in the Middle East (1948 to 1982); Eritrean refugees in Sudan (1974 to 1991); and Iraqi refugees in Jordan and Syria in the 2000s. The supplemental cases were internally displaced people in China in the 1930s, southern Sudanese in Kenya, Burundians in Tanzania, and Liberians in Ghana. Sude et al. 2015, pp. 3-4.
10 Ibid., pp. 4-6
11 The UNRWA continues to aid about 5.6 million eligible Palestinian refugees today, one third of them in 58 recognized camps.
12 United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA), ‘Who are Palestine refugees?’ UNRWA, as of 10 June 2020. Available at: https://www.unrwa.org/palestine-refugees. For current numbers see also from UNRWA, ‘Who we are,’ UNRWA. Available at: https://www.unrwa.org/who-we-are.
13 Note that the information on the status of Palestinians in Lebanon, Jordan, and Syria in this paragraph predates 2011, when the Syrian civil war broke out.
16 After the period discussed here Iran began to restrict significantly Afghan refugees’ movements. Farzin, Farshid and Jadali, Safinaz, ‘Freedom of movement of Afghan refugees
in Iran,' *Forced Migration Review*, 44, September 2013, pp. 85–86. Available at: https://www.fmreview.org/detention/farzin-jadali.


21 Mullins 2019, p. 137.


26 Crisp 2000, p. 613.


29 Sude et al. 2015, p. 17.

30 Mullins 2019, p. 124.

31 Sude et al. 2015, p 13; citing in part Langenkamp, op. cit. p. 233.


40 El Ghali 2019, p. 2.
41 ICG 2019, p 23.
42 Sude et al. 2015, p. 13, citing Interview number 5, March 2015.
43 Gatopoulos, Derek and Thanassis Stavrakis, ‘Migrants on the island of Lesbos find refuge on soccer field,’ AP News, 17 May 2019. Available at: https://apnews.com/article/ab4b1e92c8824f7ca029336b0f0e053c.
46 Sude et al. 2015.
49 ICG 2019, p. 9.
52 Mullins 2019, p 78.
56 ICG 2019, p. 20.
57 UNHCR, 3RP, 2018 pp. 3, 6, 10.
59 Anderson, Jessica, ‘Reimagining the Refugee Camp,’ Foreign Policy, 11 January 2016.
60 UNHCR, 3RP 2019, p. 12.
61 Rafiq and Malik 2017.


67 Bakker, Linda et al., ‘The Importance of Resources and Security in the Socio-Economic Integration of Refugees. A Study on the Impact of Length of Stay in Asylum Accommodation and Residence Status on Socio-Economic Integration for the Four Largest Refugee Groups in the Netherlands,’ International Migration & Integration, 14, 2014, pp. 431-448; published online 23 July 2013, pp. 434, 441.

68 Mullins 2019, p. 137.

69 Heery, Niamh, ‘“We’re not talking about this enough”: Ireland warned to take action against radicalization,’ from a [video], The Journal.ie, 17 March 2018. Available at: https://www.thejournal.ie/radicalisation-and-integration-in-ireland-3905160-Mar2018/.

70 Schmid 2016, p. 44.


72 Associated Press, ‘UN quota refugees had terror links: Norway PST,’ The Local.no, 2 June 2015. Available at: https://www.thelocal.no/20150602/un-quota-refugees-had-terror-links-norway-police.


75 Schmid 2016, p. 40.

76 Koser and Cunningham 2017, p. 8; Bakker et al. 2013, pp. 433, 434.

77 Iglesias, Juan et al., ¿Acoger sin integrar? El Sistema de Acogida y las condiciones de integracion de personas solicitantes y beneficiares de proteccion internacional en Espana’ [Hosting without integrating? The Reception and Integration System and the integration conditions of the refugee population in Spain] La Cátedra de Refugiados y Migrantes Forzados de la Universidad Pontificia Comillas, el Servicio Jesuita a Migrantes, y el Instituto de Derechos Humanos Pedro Arrupe de la Universidad de Deusto, February 2018, pp. 20, 26-27. Available at: https://sjme.org/wp-content/uploads/2018/02/Acoger-sin-integrar5.pdf.

78 Sude et al. 2015, p. 18; Dinçer et al. 2013, p. 17

79 Bakker 2013, p. 434.

80 Iglesias, Juan et al. 2018, p. 13
84 Dinçer et al. 2013, p. 19.
85 ICG 2019, pp. 12, 15.
86 Ibid, p. 15.
87 Iglesias et al 2018, p. 22.
88 “Sacred values” (religious or secular) are “immune or resistant to material tradeoffs” and associated with “duty-bound” reasoning; they sometimes demand “costly sacrifices” to protect them. Pretus, Clara, et al., ‘Neural and Behavioral Correlates of Sacred Values and Vulnerability to Violent Extremism,’ Frontiers in Psychology, 9 (2462) December 2018, pp. 1-2.
89 ICG 2019, p. 9.
90 Heil 2017, p. 2.
91 Pinto 2018, pp. 20-21.
92 The publication, developed with the FBI and the Department of Homeland Security and in consultation with academic and intelligence specialists, stresses that the factors are “minimally diagnostic on their own” and should be assessed as part of a “totality of circumstances”. U.S. Government, Office of the Director of National Intelligence, ‘Homegrown Violent Extremist Mobilization Indicators,’ National Counterterrorism Center, 2019, p. 21. Available at: https://www.dni.gov/index.php/ntc-newsroom/ntc-resources/item/1945-homegrown-violent-extremist-mobilization-indicators-2019.
93 Heery 2018, citing Ajmal Hussain, Research Fellow in Sociology at the University of Manchester.
95 Ibid., p. 819.
96 Silove, Derrick et al., ‘The contemporary refugee crisis: an overview of mental health challenges,’ World Psychiatry, 16(2), June 2017 p. 131.
102 Mullins 2019, pp. 102, 126-127.


Van Wijk and Bolhuis 2017, pp. 38, 47; Mullins 2019, pp. 122-123.


Warrell, Helen, ‘Inside Prevent, the UK’s controversial anti-terrorism programme,’ Financial Times, 24 January 2019. Available at: https://www.ft.com/content/a82e18b4-1ea3-11e9-b126-46fc3ad87c65.


Mercy Corps 2015, p. 37.

Bibliography


Ghali, Hana, ‘indoctrination in Beirut, Policy Brief No.2/2019.’
Gatopoulos, Derek and Thanassis Stavrakis, ‘Migrants on the island of Lesbos find refuge on soccer field,’ AP News, 17 May 2019; available at: https://apnews.com/article/ab4b1e92c88247ce0a29336b0f0e053c. Heery, Niamh, “‘We’re not talking about this enough’: Ireland warned to take action against radicalization,’ [video], The Journal.ie, 17 March 2018. Available at: https://www.thejournal.ie/radicalisation-and-integration-in-ireland-3905160-Mar2018/.


Hierro, Lola, ‘¿Qué necesitan los refugiados para integrarse en España?’[What do refugees need to integrate into Spain?] El País, 15 February 2018. Available at: https://elpais.com/elpais/2018/02/14/migrados/1518608962_915268.html.


Schmid, Alex P. ‘Links between Terrorism and Migration: An Exploration,’ the *International Centre for Counter-Terrorism – The Hague (ICCT)*, 7(4), 2016.

Silove, Derrick, Peter Ventevogel, and Susan Reed, ‘The contemporary refugee crisis: an overview of mental health challenges,’ *World Psychiatry*, 16(2), June 2017, pp.130-139.


United Nations Relief and Works Agency (UNRWA), ‘Who are Palestine refugees?’ UNRWA, as of 10 June 2020. Available at: https://www.unrwa.org/palestine-refugees.

United Nations Relief and Works Agency (UNRWA), ‘Who we are,’ UNRWA, 2020. Available at: https://www.unrwa.org/who-we-are.

University of British Columbia, ‘LLTD: Dadaab Camps,’ University of British Columbia. Available at: http://lltd.educ.ubc.ca/media/dadaab-camps/; also: https://refugeereview.wordpress.com/2013/08/06/borderless-higher-education-for-refuges/.


Warrell, Helen, ‘Inside Prevent, the UK’s controversial anti-terrorism programme,’ *Financial Times*, 24 January 2019. Available at: https://www.ft.com/content/a82e18b4-1ea3-11e9-b126-46fc3ad87c65.


Web-based Resources

Combating Terrorism Center at West Point. Available at: https://ctc.usma.edu/.
European Asylum Support Office. Available at: https://easo.europa.eu/.
European Commission, Erasmus Plus Programme. Available at:
Radicalisation Awareness Network. Available at:
https://ec.europa.eu/home-affairs/what-we-
do/networks/radicalisation_awareness_network_en.
United Nations High Commissioner for Refugees (UNHCR.org):
By Situation (interactive), for example. Available at:
https://data2.unhcr.org/en/situations/syria#ga=2.189021615.521349698.1569017007-
597230346.1563487066.
United Nations, International Organization for Migration: Available at:
https://www.iom.int/.
University of Oxford, Migration Observatory. Available at:
https://migrationobservatory.ox.ac.uk/.
U.S. Government, National Institutes of Health, National Center for Biotechnology
Information. Available at: https://www.ncbi.nlm.nih.gov/pubmed/.
U.S. Government, Office of the Director of National Intelligence, National Counterterrorism
Center. Available at: https://www.dni.gov/index.php/netc-newsroom/netc-resources
Chapter 10

Preventing Terrorism from Students of Extremist Madrasahs: An Overview of Pakistan’s Efforts

Asad Ullah Khan and Ifrah Waqar

Historically, madrasahs as religious teaching institutions have held a position of esteem and significance in the Indian subcontinent. Since Pakistan’s independence, madrasahs have played a significant role in not only providing religious education, but also offering free board and lodging to many of the country’s poorest children. Overtime, their numbers have grown, owing to a number of national and international factors. After 9/11, a debate on regulating madrasahs and their curriculum gained strength, as links connecting extremist and terrorist elements operating in the country with these institutions were found. A number of government measures to introduce reforms and regulate madrasahs in Pakistan have been announced to date, but have mostly been unsuccessful - largely due to a lack of political will. This chapter examines the evolution, landscape, and features of the current madrasahs system and efforts to streamline them, the obstacles in their implementation, along with an overview and evaluation of Pakistan’s counterterrorism strategies related to madrasahs and, to a lesser extent, mosque reforms. The social setting of madrasahs and their role in education, politics, radicalization and terrorism is also discussed in some detail.

Keywords: madrasahs, radicalization, religion, extremism, terrorism, education, reforms, mosque, Pakistan
Madrasah (religious seminary; plural: madrashas or madaris) is an Arabic word which literally means a certain type of educational establishment. It is one of the oldest Muslim institutions and its purpose is to teach and impart knowledge and wisdom to members of society. Madrasahs have existed in the sub-continent for a long time. During the colonial rule of the British, the Ulema (religious leaders) and their madrasahs played a leading role in the resistance against imperialism. When Pakistan became independent in 1947, around 247 religious seminaries existed. Until the 1970s, they were viewed as peaceful educational institutions working for the betterment of society in Pakistan. Many of the older madrasahs had well-established reputations for producing serious Islamic thinkers, while others provide welfare services to the poor by offering their sons free religious education, lodging, and food.¹

However, after the Soviet invasion of Afghanistan, the purpose of these religious institutions was diverted intentionally to resist Russian influence by waging a jihad against the foreign occupation forces. During that time, around 1,000 madrasahs were established². The mushrooming growth of madrasahs in the 1980s was linked to the Afghan war. A Jihadi mindset emerged in madrasahs as the US and Saudi Arabia were funding the mujahedeen against the Soviet occupation. However, in the late 1980s, the US suddenly withdrew from the region after the Soviet withdrawal from Afghanistan. Pakistan was left alone to deal with the seeds of radicalization sowed in its home and backyard. This vacuum led to the growth of radical and extremist tendencies and mindset in Pakistan, especially in the madrasahs. The phenomenon of Talibanization also took roots. Consequently, this created hatred and resentment among the radicalized youth of madrasah in Pakistan and they began to consider the West as a threat to, and enemy of, Islam.

In the aftermath of the 9/11 attack by Al-Qaeda, Pakistan was pressed hard by the US to take part in the Global War on Terror (GWOT) which once again brought madrasahs into the limelight, but this time their perceived image was negative. Western policymakers criticized madrasahs and held them responsible for fuelling extremism in society. Pakistan’s decision to join the GWOT changed the social and security landscape of Pakistan. It also led to a renewed debate in Pakistan about the role of madrasah and the need for reforming the more than 37,500 Madrasahs currently operating in Pakistan.

It is no secret that madrasahs have a political role in society as well. Major religious political parties have their own network of religious seminaries which they run by funding them. These religio-political parties often use their madrasahs and their students for political purposes or to pressure governments through staging protests. Hence, the socio-political impact of these religious seminaries cannot be ignored; they have long-term consequences. There is also a great deal of controversy as to what type of role madrasahs ought to perform in society.³ According to Christopher Candland, it is the government which needs to recognize and determine madrasahs’ role in society by giving them appropriate attention.⁴ Yet that is easier said than done. Qasim Zaman has highlighted repeated failures in reforming madrasah and attributed these to radical elements in Pakistani society who sought to boycott the government’s reform agenda.⁵ A number of steps to reform madrasahs in Pakistan have been taken in the last two decades, but they have indeed achieved much less than one could expect due to a lack of political will and stiff resistance from religious circles. However, from 2010 onwards, the country’s counterterrorism strategy has led to a renewed focus on madrasah reforms. Mapping, streamlining and regulating the religious seminaries have been the buzzwords on policy agendas. However, it has also been observed that the phenomena of terrorism and extremism cannot be attributed to madrasahs and their students alone, since there have been a number of instances where college educated individuals have become radicalized and have taken part in terrorist acts. This chapter seeks to examine the role of madrasahs in radicalization to violent extremism and the government of Pakistan’s prevention efforts.
**Evolution of Madrasahs in Pakistan**

The growth of religious seminaries in Pakistan should be seen in the light of political and socioeconomic factors. When Pakistan became independent on 14 August 1947, only 247 madrasahs existed, according to official figures. In 1975, there were 100,000 seminary students in Pakistan; in 1998 their number stood between 540,000 in Punjab alone. In the 1980s, Pakistan’s support for the US against the Soviet Union turned the madrasahs from hubs of education to centres promoting Islamic extremism. As mentioned before, their number mushroomed during the Soviet-Afghan war. Pakistan bore direct consequences of the Afghan war as the country played a major role in resisting the Soviet occupation of Afghanistan. Religion was used as a tool, as the Afghan War was termed by Pakistan’s military ruler General Zia-ul-Haq as jihad (holy war). During Haq’s tenure (1978-1988), the number of religious seminaries increased to 2,831.

General Zia was politically allied with Islamist parties. He encouraged them to motivate their members to join this “holy war” against the Soviets. The clout of these religious parties grew multi-fold during the 1980s as they enjoyed both religious and political backing. Afghanistan’s Taliban movement has roots in these religious seminaries, as a number of Taliban leaders were educated there. Many of Pakistan’s religious parties translated their influence on the ground by opening their own madrasahs. They often received funding from both the West and the countries of the Gulf Cooperation Council (GCC) for providing education to the children of millions of Afghan refugees who had fled war in Afghanistan.

Although the Afghan war ended in the late 1980s, the number of religious seminaries continued to increase. This increase in their numbers is also attributed to various socioeconomic reasons. These religious seminaries provide free board and lodging to their students, and it is tempting for the economically downtrodden to send their children there. According to Pakistan’s military spokesperson, more than 30,000 madrasahs are operating in the country, in which an estimated two and half million children are currently enrolled. However, according to a study conducted by a Karachi-based research centre, the Majlis-e-Ilmi Foundation Pakistan, the number of madrasahs in the country is even higher, exceeding 37,517 in 2018 as seen in their image below. According to the statistics released by this research centre, 28,241 madrasahs are functioning under the five central boards of the Ittehad-e-Tanzeem-ul-Madaris Pakistan (ITMP), whereas the remaining 9,276 are operating under different independent bodies which include Jamaat-ud-Dawa, Jamia Muhammadia Ghausia, Itihad-ul-Madaris, Wafaq Nizam-ul-Madaris, Al-Huda International, as well as others. According to the foundation’s report, 354 madrasahs are operating in Islamabad, 13,798 madrasahs in Punjab, 10,033 in Sindh, 2,959 in Balochistan, 3,579 in Khyber-Pakhtunkhwa, and 1,404 in Azad Jammu Kashmir.

**Landscape of Madrasahs and their Impact in Society**

There is no doubt that madrasahs are considered to be important institutions in Islamic societies, but this also applies to mosques. Besides worshipping, the mosque traditionally has held the title of seat of learning - in addition to being a community centre in Muslim societies. Similarly, the madrasah has historically been considered not only as a source for imparting religious education to the masses, but also for training and equipping imams (religious leaders) and for their role in mosques. The religious leaning of these imams is very much dependent upon the thinking of madrasah or from the sect they belong to.

Historically, society’s elite used to study in these religious institutions, but today, due to the prevalence of formal education systems and modernization, the mosque and madrasahs have become merely political tools for the elite. Religious leaders, politicians, and even those
holding state power do not hesitate to use these institutions and the name of religion for advancing their own political agendas and gains.

Madrasah’s affiliations with political, sectarian and militant organizations affiliations with madrasahs are a cause for concern. Such affiliations may drive their administrations and their students towards assuming an increased role in society. Friday sermons from the mosque are an important event for the Muslim community as Muslims listen to the narratives of imams on various religious and social topics. These sermons play an important role in shaping the public opinion regarding various issues in daily life. In addition, the interaction between people and imam five times a day during prayers further enhances the impact of his words and affects people’s psyche. Since the imam’s sermons are monitored, he is careful with his words and the speeches he delivers to the public.

The donors of the religious seminaries are businessmen, social workers, and other society members. This relationship is considered very strong, as it is believed that making an economic contribution to religious causes is beneficial for both donors and recipients.

Nowadays, with the increasing number of madrasahs in society, some donors use madrasahs to get appropriate legal verdicts (fatwa) on different social issues to advance their personal and sectarian interests. However, it is hard to establish proof regarding influencing verdicts. For instance, the Punjab police need the assistance of intelligence agencies as well as the Federal Investigation Agency (FIA) to collect solid evidence against corrupt seminaries for possible legal action. Over 12,000 seminaries are operating in Punjab alone, with almost half of them being unregistered.

A misperception exists in the society that madrasahs are entirely charity-based organizations. For the most part, they are associated with one of five religious educational boards, which are sectarian in orientation. On the other hand, religious seminaries consider themselves as non-governmental organizations (NGOs). Many of the madrasahs now own property and are making investments for profit.

The Madrasah System in Pakistan

Madrasahs in Pakistan mostly belong to the two major sects of Islam i.e., the Sunnis and the Shias. Sunni Islam is further divided into three sub-sects: Deobandi, Barelvi, and Ahl-i-Hadith. Apart from these, some religio-political parties like Jamat-e-Islami, run their own madrasahs.
In order to oversee the educational curricula being imparted in these madrasahs, five independent boards were established, based on these different sects. These boards are responsible for finalizing the syllabus, conducting examinations and awarding degrees in the respective madrasahs. Pakistan’s Higher Education Commission recognizes the degrees awarded by its approved Wafaq/Tanzeem ul Madaris. Following are some of the details of the Central Board of Madrasahs in Pakistan.

Wafaq ul Madaris: The largest number of Islamic seminaries globally are run by Wafaq-ul-Madaris Al-Arabia in Pakistan. It has its headquarters in Multan. From its inception in August 1959, the total number of madrasahs working with Wafaq-ul-Madaris grew to 19,491 by August 2018. More than 8,000 Iqra Schools and 10,000 seminaries from around the country are associated with it. It is affiliated with the Deobandi school of thought. It has an approved syllabus, conducts regular examinations, and awards degrees to its students.

Tanzeem ul Madaris: The Tanzeem ul Madaris was established in 1960. Its headquarters are in Lahore. It represents the Barelvi school of thought. About 10,000 madrasahs associated with the Barelvi exist in the country. In 2019, more than 200,000 students attended examinations under the Tanzeem ul Madaris.

Wafaq ul Madaris (Shia): The Wafaq ul Madaris (Shia) came into being in 1959 in Lahore. It is associated with the Shia school of thought. The board has its own syllabus, conducts its own examination regularly, and awards degrees.

Rabta-tul-Madaris-al-Islamia: The Rabta-tul-Madaris-al-Islamia was formed in 1983 by the revivalist religio-political party of the country Jamat-e-Islami (JI), but the board was only recognised by the government of Pakistan in 1987. Since its inception, the JI has stated that its education board is not affiliated with any sect or group. Subjects of politics, economics, and history are taught in their madrasahs, along with traditional Quranic education in their bid to modernize their education system. Its headquarters are located in Mansoora, Lahore.

Wafaq-ul-Madaris-al-Salafia: The Wafaq-ul-Madaris-al-Salafia, formed in 1955, caters to the Ahl-i-Hadith school of thought. They adhere to Quran and Hadith very strictly and have their own system of examination and awarding degrees.

The largest association of seminaries in the country is the Ittehad-e-Tanzeemat-e-Madaris Pakistan (ITMP) also known as the Union of the Religious Education Organizations. It was formed in 2005. Five constituent boards came together to form the ITMP to effectively negotiate with the government.

Analysis of The Curriculum of Madrasahs

When the role of madrasah as a teaching institution is being analyzed, one cannot ignore the importance and relevance of the curriculum being taught in the seminaries. The curriculum currently being taught in the seminaries is called Dars-e-Nizami. It was developed by an 18th century scholar, Mulla Nizamuddin Sihalwi, from the Farangi Mahal madrasah, located in the now Indian city of Lucknow. Traditional madrasahs adhere to it except for those of the Shia part of the population. The text of its syllabus dates back 500 years or more. Owing to the inability of the majority of students to understand Arabic texts, this course is taught with the help of commentaries and interpretations done by medieval scholar Hanafi Ulema. The original text is memorized by students, often without a complete understanding of the context or the meaning. As a result, students are unable to develop analytical abilities, and grow up with a narrow understanding of the scripture and the world. This fact has been highlighted by local scholars who opine that this traditional technique of learning and teaching at madrasahs should be changed, as it reflects a stagnation of knowledge.

Another problem with the curriculum being taught at religious seminaries is the issue of of animosity towards other schools of thought, both secular and religious. With a curriculum that is suspected of glorifying violence in the name of Islam while ignoring basic history, science
and math, that part of Pakistan’s public education system has become a major barrier to defeat extremist groups.21 As Rebecca Winthrop and Corninne Graff noted, the majority of madrasahs do not impart any secular or vocational training, but they have rigid curricula emphasizing rote memorization. It has been argued - albeit based on limited evidence - that they deliberately educate their students in narrow worldviews and the rejection of Western ideas, and do not train them sufficiently for the real world.22 Injecting advanced subjects and modern research in the curriculum could bring this system at par with the modern educational system.

There are two major issues with the curriculum of madrasahs. Firstly, the rigid interpretation of all the concepts according to the doctrine of a particular sect and school of thought, which considers all other interpretations as inauthentic. This tends to spread hate and divisions in society. Secondly, the concept of jihad in Quran and Hadith is arguably misinterpreted and misunderstood in the existing curriculum: it urges students to embrace militancy when it comes to spreading their faith, which is not the true concept of jihad.

The curriculum needs to be revamped in this regard in order to eliminate this kind of interpretation. Political will and intent needs to be displayed to enforce the necessary changes on the ground. This process will take time but in the long run should prove beneficial to both students and the state.

**Prospects of Reforms**

Contrary to popular notions, the drive to bring reform to madrasahs in Pakistan precedes the events of 11 September 2001. In fact, then Army Chief and President General Pervez Musharraf wanted to limit the influence of these religious institutions. The National Education Policy 1999-2000 encompassed a reform program for madrasahs which the government wanted to implement. It included bridging the existing gulf between formal education and the education offered by madrasahs; equating their scholastic achievement degrees with the ones of the formal education system; recognizing them and providing them with books on research and reforms; and striving for an integrated system of national education.23

In line with this policy, certain steps were taken which included *The Pakistan Madrasah Education Board Ordinance, 2001.* This ordinance, promulgated on 18 August 2001, sought to “secure registration, regulation, standardization and uniformity of curricula and standard of education of the dini (religious) madaris, imparting specialized Islamic education in Pakistan with the general education system.”24 Unsurprisingly, this ordinance could not achieve its objectives mainly due to the lack of enforcement and opposition from religious circles.

**Implications of 9/11 and Madrasah Reforms**

The events following the attacks of 11 September 2001 led to a number of developments. Renewed attention was given to madrasahs, their structure, curriculum, and working. Demands for reforms started building up, as non-reformed madrasah operating outside the ambit of the state were widely seen as training grounds for terrorists and extremists. Nevertheless, the government of Pakistan faced stiff resistance from conservative religious clerics who viewed the proposal to reform madrasahs as a Western move to control or alter the religious teachings of Islam.

**Madrasah Reform Program**

In 2002, the government of Pakistan launched the “Madrasah Reform Program” (MRP). MRP was said to be a five-year program to mainstream 8,000 madrasahs with a budget of Rs 5,729.395 million.25 The Ministry of Education was tasked with introducing subjects like
English, general science, and mathematics at the primary level, and then teach computer science, economics etc. at the secondary level, in order to bridge the gap between the different educational systems existing within the country. It also included steps to increase interaction between formal and informal education systems of education as well as equipping madrasahs with computers. However, the reform program was not successful, due to the lack of capacity to utilize funds as well as the lack of implementation and coordination. Secondly, the madrasah leadership was hesitant to trust the Ministry of Education, and there was friction with the Ministry of Religious Affairs.

In 2005, the “Madrasahs Voluntary Registration and Regulation Ordinance” was issued by the government, seeking to bring madrasahs under the supervision of the state. It stated that no madrasahs would be able to function without registering themselves. They were also tasked to submit audit reports on their organization. In addition, the 2005 ordinance called for putting an end to hate speech which incited sectarian or religious tensions.

Post National Action Plan, 2014

A standard mechanism of registration of madrasahs was drafted after consultation with the ITMP and the National Counter Terrorism Authority (NACTA) in the National Action Plan (NAP) document. It was observed that more than 190 madrasahs were foreign funded. Similarly, 182 madrasahs were closed down immediately as they were found to promote militancy in the country and to have connections with militants and proscribed organizations. There is still a long way to go as mere registration of madrasahs will not be enough. Since the madrasah system is not getting any direct assistance from the government of Pakistan, little control can be exercised. It is a well-established fact that donors always influence the receiving institutions. Government should arrange extensive training programmes for teachers and those who qualify should get some special pay package. The system should be controlled federally at the initial stages, and then it may be delegated to the provinces once the desired results are achieved. Initially the central government could set up some model madrasahs in big cities and that role model could then be applied uniformly in other parts of the country.

Resistance to Reforms?

On the national level, there is public support to streamline madrasahs and introduce reforms, however, the government faces resistance in this regard. The pushback comes mainly from the powerful religious parties who run a network of madrasahs, but do not want any government involvement. There have been numerous attempts to bring reforms to streamline madrasahs, but they were unsuccessful mainly due to the stiff resistance from conservative circles and a lack of political will.

Madrasahs and their Impact on Society

Madrasahs see themselves as custodians of the teachings of Islam as they provide free education and shelter services to society. Madrasahs face a multitude of challenges in preparing students for life in rapidly modernizing societies and emerging globalized knowledge economies. There are multiple factors that lead to producing an extremist and radicalized mindset in the madrasahs, including economic vulnerability, social divisions and discord, sectarian differences, using religion for political purposes, and misinterpreting religion - especially the concept of jihad.

Jihad has been used by fundamentalists, with varying intensity, as a unifying and energizing force. In some madrasahs, the minds of students are radicalized in such a manner
that they are ready to participate in acts of violence, which they see as their religious duty. Madrasah students are sometimes told that it is their duty to stop any “immoral” activity and raise arms against any entity which deviates from the righteous path. By such indoctrination, vulnerable young minds are prepared to join the “Holy War.” In addition, the leaders of some of these sectarian outfits incite their followers and students through hate speeches and literature to create disharmony in the society.

Madrasah and Politics

The affiliation of madrasahs with religious political parties can be traced back to the inception of Pakistan. Before the era of 1980, religious political parties were running madrasahs as charity-based organizations and as a service for society. After the decade of the 1980s, many madrasahs heavily focused on a jihad-oriented curriculum. In addition, sectarian differences were emphasised in these religious institutions, as most of their funding was originating from Sunni-majority countries in the Middle East. This led to an increase in radicalization and polarization in society.

The religious political parties also divided themselves on the basis of sects, and extended their presence in madrasahs. It resulted in a politicization of these religious institutions, and the original purpose of imparting religious education has been largely lost. According to a survey conducted by the Pakistan Institute of Peace Studies, a majority of the madrasahs have an affiliation with political parties. The majority of these religious seminaries are themselves also eager to play a role in politics, e.g., by supporting candidates in elections. For example, Azhar Husain Rizvi, an independent candidate backed by Labbaik Ya Rasulallah, a coalition of Islamist groups, won six percent of the vote by campaigning on a platform supporting strict blasphemy laws. It is pertinent to note here that the involvement of madrasah students in politics distracts them from their primary objective of education. This affiliation leads to a rigid mindset, and eventually results in the formation of extremist narrative. Affiliation with any single political party or sect, makes students unable to think beyond party lines.

Streamlining Madrasahs

Pakistan has been grappling with terrorism and violent extremism for more than a decade. The country has suffered immense physical and economic losses due to these phenomena. Over the years, the demand to take strict measures to eliminate terrorism and extremism has not only arisen domestically, but there has been a significant international pressure on Pakistan in this regard as well. Since the number of terrorist attacks increased in the country, especially after 2001, it was repeatedly found that most of the perpetrators were madrasah students who had been coerced into picking up weapons. As more details about this connection started to emerge, emphasis on the need for streamlining madrasahs also arose. There have been a number of proposals, institutions, and policies suggesting reforms in the last two decades, but limited success in this domain has been achieved.

The Current Situation of Madrasahs

Serious work towards registration and regulation of madrasahs started after the NAP. The current government of the Pakistan Tehreek-i-Insaf (PTI) party - which took reins of the country in 2018 - announced in an election manifesto that it would “map out and register all seminaries across Pakistan including information on finances, and introduce literacy and mathematics teaching as formal subjects within the madrasah curriculum.” Since taking power, PTI has made some headway in this regard. In March 2019, the government announced
that it had assumed control of 182 religious schools, and detained 182 people in its bid to take strict action against banned groups.\textsuperscript{34} Furthermore, the (now former) spokesperson of the military, Major General Asif Ghafoor, said during a media talk, “The government of Pakistan ... has decided that these madrasahs will be mainstreamed.”\textsuperscript{35} He further added that in this drive, the country plans to take control of over 30,000 madrasahs where over 2.5 million children are studying, and introduce a modern educational curriculum so that the children studying in these religious institutions will be well equipped to deal with the contemporary world.

The current curriculum format of (the majority of) madrasahs is still mainly based on memorization of the Holy Quran. As a result, madrasah students remain behind in terms of practical skills when compared with those who have studied in colleges and universities. Madrasah graduates have very limited employment opportunities as almost the only work they can find - if they are lucky - is to teach Islamic studies or Arabic in schools or become madrasah teachers themselves. Some become imams, but the majority remains unemployed and become frustrated owing to the lack of employment opportunities. As a result, a socio-economic division is created in the society which creates disharmony, and is a threat to national cohesion. Another challenge for the state of Pakistan is to control hate speech, as madrasahs often serve as a breeding ground for radicalization and the development of extremist tendencies, especially where vulnerable young minds are concerned. They are used by militant outfits for their own ends in the name of religion. However, it should be remembered that most madrasahs are not involved in any illicit activities. As Major General Ghafoor said, “just 100 madrasahs have been found involved in violent activities, while the rest are a good and effective source of education for children.”\textsuperscript{36}

In May 2019, the country’s Education Minister, Shafqat Mahmood met with the leaders of the country’s five Madrasah boards, to carry forward the process of reforms, and place them under the supervision of the Ministry of Education. The minister also promised to assist madrasah operators in opening bank accounts, the registering process, as well as providing help in processing visas of foreign students who seek admission there. The spokesperson of Wifaqul Madaris Al-Arabia (one of the five Madrasah boards), Maulana Ibrahim Sakargahi said, “It was our long-standing demand that the responsibility[...]should be given to the Education Ministry.”\textsuperscript{37}

Funding to Streamline Madrasahs

One of the biggest issues ahead of streamlining madrasahs is to ensure their financing. Pakistan, which is already in the middle of an economic crisis, has expressed its intent to bear the financial burden of major madrasah reforms. Major General Ghafoor said “Pakistan would pay for the madrasahs by diverting cash to education from the cost of anti-terrorism security operations, which are less necessary because militant attacks have sharply declined in recent years.”\textsuperscript{38} A senior official from the Ministry of Education echoed the military spokesman’s statement and said that “the government will bear the financial burden to introduce these major reforms in Madrasahs which are a major source of education for poor children.”\textsuperscript{39} These statements are indeed heartening, and signals an intent of the state of Pakistan to take out spoiler elements from the society.

Madrasahs and Terrorism

There are two broader aspects of terrorism when one looks at these through the lens of madrasah reforms. First is the transnational, and the second is the homegrown form of the
terrorism. There is a widespread perception in the country that the renewed friendship with the US following the 9/11 attacks was being driven solely by America’s need for Pakistani cooperation in the Global War on Terror.40

Western experts on this subject link transnational terrorism to global jihad, and consider it a threat particularly targeting the West. However, the facts on the ground offer a different picture. No major attack carried out in the West has been traced back to anyone who attended a Pakistani madrasah. However, according to a report of the UN Security Council Monitoring Committee on Al-Qaeda in May 2020, up to 6,500 Pakistani nationals currently fight in Afghanistan on the side of the Taliban against government forces and their foreign backers.41 In general, madrasahs in Pakistan have been more involved in domestic sectarian violence than in transnational activities after the withdrawal of the Soviet Union from Afghanistan. Yet the domestic impact has been significant, especially in the more isolated parts of the country which have the highest potential for radicalization.42 The issue became prominent with the emergence of Tehreek-i-Taliban Pakistan, an organized terrorist group whichescalated sectarian tensions in the country as it mostly targeted the Shi’ites.

In addition, some madrasahs in the (former) tribal areas played an important role in hiring vulnerable young people and training them to be terrorists. It has been observed that the seminaries which had ties with proscribed organizations were often involved in facilitating terrorist attacks in Pakistan. At least 299 madrasahs have been found to be involved in terrorism and sectarian activities in Punjab alone.43 Terrorists often take refuge in certain seminaries where they have also been caught many times. There is a very close link observed between certain religious institutions and sectarian violence. All Muslim sects happily claim that their sect is the naji (“saved one”) and the “others” are destined for hell.44 This division, based on ideology and religious arguments is a major obstacle when it comes to drafting a reform plan that can be applied uniformly to all madrasahs in Pakistan.

Some madrasahs in Pakistan pretend to be working as national universities and claim that they can discuss Islamic jurisprudence to promote harmony in the society. Their claim is difficult to validate. They do not promote religious pluralism; rather their efforts revolve around the rejection of other schools of thought and the promotion of their particular school of thought. This sectarian divide is perhaps the biggest hurdle when it comes to reforming the process of education.

An Overview of Pakistan’s Post-9/11 Counterterrorism Strategies Regarding Madrasah and Mosque Reforms

The events following the 9/11 attacks brought global attention towards the alleged role of madrasahs, and led to a discussion on their impact. As the War on Terror evolved, there was also a gradual increase in terrorist activities inside Pakistan. Some of those terrorist attacks against the state and its institutions in Pakistan were conducted by people who had been informally schooled and indoctrinated in madrasahs to act against the state and its institutions. This led to renewed calls of regulating all madrasahs operating in Pakistan. Almost all sections of society started calling for the need to scrutinise their financial channels, regulating their syllabus, and register them so that a better eye could be kept on these seminaries. Madrasahs were viewed by many people as a backward educational institution and its students were looked down upon by those who received their education in formal schools. Calls for reform grew stronger. For this purpose, many policy proposals and rounds of talks were held between officials and the ITMP, but they could not achieve a consensus. Ultimately, the National Internal Security Policy (NISP 2014-18), then the NAP (2014), and then the second National Internal National Security Policy (2018-2023) formally included regulation, reform, and mainstreaming of madrasahs as specific agenda items.45

The NISP 2014-18 was Pakistan’s first ever national security document. The 64 points in the policy were approved by the federal cabinet in 2014. The scope of the report was defined to be focused on internal security. A need for developing a national narrative was also highlighted in the report to counter non-traditional threats with the help of religious scholars, the intelligentsia, educational institutions, and the media. For the first time, the NISP 2014-18 categorically stated that the “Madrasah system cannot be excluded from the internal security parameters of the country.”

Five issues were addressed:

1. **Identification of root causes inside madrasahs involved in radicalization:** The NISP 2014-18 clearly stated that some madrasahs were involved in spreading extremism inside the country. As madrasahs usually have an outdated curriculum, the students which passed from these informal centres have limited employment opportunities as opposed to those with formal education. This factor led to the breeding of contempt and frustration among the vulnerable madrasah-educated youth. They were more prone to anti-state elements who could misuse or radicalize them. Initially, this observation was limited only to boys studying in these madrasahs, but “after the Jamia Hafsa incident has brought madrasahs for women also under the microscope of security analysts.” The document highlighted how madrasahs were competing with each other for influence in the country. The complete rejection of other beliefs and sectarian indoctrination plays, according to the NISP 2014-18, a critical role in dividing society and adding emotive fuel to existing divisions in the society. Therefore, madrasahs and mosques remain important focal points for the government to stop the flow of violent extremism in the country, as a number of terrorists were madrasah students.

2. **Mapping, integrating, and mainstreaming mosques and madrasahs:** Most of the madrasahs involved in radicalization operate outside the realm of government structures and national law. The main target of extremists, terrorists, and anti-state elements are national integration and harmony. The policy document called for mapping the existing as well as new madrasahs and mosques as it would help in mainstreaming them with the rest of the educational institutions in the country. NISP 2014-18 called to “include broad based Madrasah and mosque integration process in the mainstream education system so that students and alumni of these institutions can also become active members of a plural society and play a positive role in the national economy being part of a productive workforce.”

3. **Stemming the financing of terrorism in the name of madrasahs:** The NISP 2014-18 emphasized “some troublesome aspects of these madrasahs, which impinge on national internal security, include financing from unidentified sources; publication and distribution of hate material.” According to the NISP, it should become possible for the Federal Board of Revenue and taxation department to distinguish between legal and illegal flow of money by involving banks in monitoring the flow of money to suspected organizations.

4. **Legal Reforms:** The NISP 2014-18 called for a review of the regulatory capacity of the state to monitor, evaluate, and prevent the misuse of existing laws under which mosques and madrasahs are functioning.

5. **NACTA’s Responsibility to Implement the NISP 2014-18:** Whereas the NISP 2014-18 called for better oversight and regulation of madrasahs and mosques, NACTA, which was established in 2009, was tasked with its implementation.

NACTA’s Directorate of Research and Coordination was, inter alia, tasked with madrasah mapping, legal reforms and policies of mosques and madrasahs related to internal security.
National Action Plan (2014)

Following the tragic attack on the Army Public School in Peshawar on 16 December 2014, in which 150 people, mostly students, were killed by the Taliban, a broad consensus was agreed upon by all major stakeholders to eradicate terrorism and clamp down on its funding and infrastructure. As a result, a 20-point NAP\textsuperscript{55} was set up. Registration and regulation of madrasahs became action point number 10 in this NAP.


Among other things, the second National Internal Security Policy document (NISP 2018-2023) emphasizes the continuing need for madrasah and mosque reforms. The report states that significant success has been achieved as far as the mapping of madrasahs was concerned, with over 90\% of religious seminaries (\textit{madrasahs}) now identified and counted. It was also noted that efforts to introduce wide-ranging madrasah reforms were well underway.\textsuperscript{56} The following elements stand out in the NISP 2018-2023:

- \textbf{A new national narrative}: A new national narrative was introduced, calling for “a tolerant, inclusive and democratic polity.” It emphasizes that cultural and religious diversity will be the most significant pillars of this narrative. Furthermore, it also states that a “comprehensive National Narrative against extremism and terrorism predicated on acceptance of plurality, diversity and tolerant teachings of Islam will be prepared and disseminated.”\textsuperscript{57} In light of this new national narrative, the curricula in schools and madrasahs would be adjusted accordingly. The Departments of Education, the Higher Education Commission and NACTA were tasked to ensure implementation.

- \textbf{Radicalization and militancy not limited to madrasahs}: The NISP 2018-2023 highlights that there is sufficient evidence indicating that radicalization and militancy is not just limited to madrasahs or its students. In fact, people from affluent backgrounds, with modern educational qualifications, are also vulnerable targets of the radical narratives.

- \textbf{Adoption of minimum national standards}: The policy document calls for an adoption of minimum national standards to be set for madrasahs as well as public and private education institutions.\textsuperscript{58}

- \textbf{Uniform registration and regularization of madrasahs}: The policy document states that a uniform registration and regularization of madrasahs in all provinces will be guaranteed, and provinces would accordingly devise legislation to undertake madrasah reforms and streamline them. Some proposed reforms for madrasahs and mosques include:

  - \textbf{Conditional State Assistance to Madrasahs}: The policy document states that State funding has to be linked with financial auditing, the adoption of a national curriculum, the teaching of science subjects, and an institutionalized examinations system;\textsuperscript{59}\textit{Assistance in Switching from Madrasah to Mainstream Education System}: It has been stated in the policy document that “avenues to switch from Madrasah to the mainstream education system will be created at a level equivalent to years 5 and 10 of schooling.”\textsuperscript{60}

  - \textbf{Increased Collaboration between Madrasah and Mainstream Educational Systems}: In order to remove misconceptions, promote harmony, and to encourage a positive exchange of ideas, increased collaboration between madrasahs and mainstream educational systems was proposed, including both student and teacher exchange programs, and joint academic as well as extra-curricular events;

  - \textbf{Mosques as Centre of Guidance and Learning}: The NISP 2018-23 also states that mosques will be reformed and made into centres of guidance and learning. In addition,
narrative and guidelines for the Friday prayer sermons approved by the government in consultation with the religious scholars should be prepared, stressing, inter alia, the importance of civic values in the sermons. A pilot program was to be launched in the city of Islamabad.

- **Training of Imams:** The NISP 2018-23 announced that “a committee of religious scholars (with representation from all schools of thought) will be established for the formulation of recommended syllabi, examination and training for Imams.” Under the supervision of this committee, and overseen by the Ministry of Religious Affairs, a special training program would be offered to imams. Furthermore, the expertise of imams would be ensured by an examination conducted by the state. The ones who qualify would be given a monthly stipend by the government.

- **Funding to Set up Libraries at Mosques and Centres for Islamic Studies:** Under the guidance of the Ministry of Religious Affairs, assisted by the committee of scholars, the policy document announced that government funding would be provided to establish libraries at mosques and centres for Islamic studies. To ensure transparency, these funds would be audited by the government.

**Evaluation of the above Counter-Strategies**

In 2014, when the first NISP (2014-18) was announced, it was considered a landmark document. These 64-point laid out comprehensive plans and reforms focusing on improving the national security situation of the country. In this policy document, NACTA was given various responsibilities to implement the action points on the ground. However, following the terrorist attack on the Army Public School Peshawar, a new 20 points action plan by the name of “National Action Plan” was adopted, and NISP was rendered inconsequential as NAP de facto took NISP’s place.

Following these two policy directives, with regard to regulating madrasah reforms two steps were taken by NACTA:

- **Madrasahs Data and Registration Forms:** In consultation with the ITMP, NACTA devised the “Madrasahs Data and Registration Forms”. The objective behind this step was that only registered Madrasahs would be allowed to operate and function in the country.

- **Curriculum and Equivalence Mechanism:** In order to revisit madrasah curricula and so as to give an equal formal status to its degrees, two committees were established. They included members from the ITMP. According to NACTA, the first committee is working under heads of Federal Board of Intermediate and Secondary Education and the second committee is working under chairman Higher Education Commission (HEC) regarding grant of equivalence certificate to Wafaq-ul-Madaris for Sanad Shahadat ul Aamawa Khasa.” Extensive deliberations have been taking place by these committees.

The second NISP (2018-2023,) like its predecessor, is extremely broad in its scope. Instead of being narrowly focused, the plan seems to be too ambitious. However, the policy document includes positive ingredients, especially regarding madrasah and mosque reforms.

The madrasah regulation reform, especially in terms of its mapping, has achieved considerable success. According to a NACTA report presented in April 2019, the geo-tagging of the majority of the madrasahs in Pakistan has been completed. 90 percent of madrasahs have been registered in Punjab, with all of them geo-tagged. In addition, geo-tagging of 85% of the madrasah in the Federally Administered Tribal Areas (FATA) has been achieved; 80% of those in Sindh; 75% of the ones in Khyber Pakhtunkhwa (KPK); 60% of Baluchistan’s madrasahs; and 100% of those in Islamabad had been completed. With this report, the government also issued a warning that all unregulated madrasahs would be closed.
remain concerns, especially regarding channelling of external financial flows to madrasahs. However, some progress has also been made in this domain.

NISP (2018-2023) was passed in the last days of the previous government. The need of the hour is that it should be given time by the new government to be fully implemented rather than giving in to the temptation to come up with a new counterterrorism strategy document of its own. Pakistan cannot afford any further delays in the domain of preventing and countering terrorism.

Conclusion

Historically, madrasahs have played a significant role in the development of the socio-political fabric of Pakistani society. Yet, it is a sad reality that over time, some of these religious seminaries deviated from their original purpose of imparting knowledge and helping the poorer and more vulnerable segment of society. They allowed themselves to become instruments of various national and international political actors and agendas. Streamlining of these madrasahs by introducing reforms, and bringing them in line with the more modern and secular national educational system of Pakistan is the need of the hour. It will not only help curb extremist and sectarian tendencies, but also benefit millions of students by enabling them to be better prepared when entering the job market. Over the years, the state of Pakistan has introduced a number of counterterrorism measures to lay a framework for reform and regulation of the religious seminaries. However, there has been a serious lack of implementation. The madrasah system has and can be an asset for Islamic societies, but it must be protected from extremist militancy. Madrasahs must be restored to their original status of educational institutions which promote Islamic core values like social harmony and moderation. All stakeholders ought to unite and prioritise this issue for the benefit and betterment of the people of Pakistan.

Asad Ullah Khan is co-author of chapter 10. He is a Senior Research Fellow at the Center for Aerospace and Security Studies. Until recently, he was a Research Fellow for Counter-Terrorism and Countering Violent Extremism at the Institute of Strategic Studies Islamabad. Asad Ullah Khan’s area of research is national security and counterterrorism. He represented Pakistan on many national and international forums on the subject matter. He is the author of numerous research articles, book chapters and opinion articles in journals, books and magazines in the domain of countering violent extremism. Mr. Khan has recently represented Pakistan at a Colombo Defence seminar in Sri Lanka and shared his research work on the forum.

Ifrah Waqar’s academic career is in International Relations. She has extensive experience of working with various national and international organizations over the past five years on issues ranging from terrorism, countering violent extremism and radicalism, foreign policy, as well as strategic and nuclear issues. She has been developing and working with the Centre for Pakistan and Gulf Studies’ CVE project, SALAM, which deals with innovative methods to address radical extremism and countering violent extremism in Pakistan. She was Project Manager for Countering Violent Extremism, under the premises of the Centre’s flagship project SALAM. In 2017, she visited the Kingdom of Saudi Arabia at the invitation of a Saudi think-tank. Ms. Waqar has also served as the Special Assistant to the Convener of Pakistan-Kingdom of Saudi Arabia Senate Friendship Group, Senator Sehar Kamran, from May 2016 till March 2018.
Endnotes

10 Ibid.
12 *Fatwa* is an authoritative legal opinion given by a mufti (legal scholar) in response to a question posed by an individual or a court of law. Available at: http://www.oxfordislamicstudies.com/article/opr/t125/e646.
Winthrop and Graff 2010.


Ibid.

Ibid.


Campbell, Alastair, ‘An Investigation into Islamic Fundamentalism and an Assessment of its Relationship with the Concept of Jihad,’ *Army Command and General Staff College, Fort Leavenworth KS*, 1992.


Anadolu Agency 2019.


Anadolu Agency 2019.


Ibid.


Pakistan Today 2019.


Anadolu Agency 2019.


Ibid.


Pakistan Today 2019.


National Counter Terrorism Authority (NACTA), ‘Madaris Reform,’ NACTA. Available at: https://nacta.gov.pk/madaris-reforms/.
Ibid., p. 39.
Ibid., p. 11.
Ibid., p. 28.
Ibid., p. 28.
Ibid., p. 8.
Ibid, p. 20.
Ibid., p. 60.
Ibid., p. 47.
Ibid., p. 48.
Ibid., p. 49.
Ibid.
Ibid.
NACTA 2020.
Ibid.
Ibid.
Bibliography


Campbell, Alastair, ‘An Investigation into Islamic Fundamentalism and an Assessment of its Relationship with the Concept of Jihad,’ Army Command and General Staff College, Fort Leavenworth KS, 1992.


Laskar, Rezaul H., ‘6,500 Pak Nationals among fighters in Afghanistan: UN,’ Hindustan Times, 3 June 2020. Available at:


National Counter Terrorism Authority (NACTA), ‘Madaris Reform,’ NACTA. Available at: https://nacta.gov.pk/madaris-reforms/.


Rana, Muhammad Amir, ‘Mapping the Madrasa Mindset: Political Attitudes of Pakistani Madaris,’ Conflict and Peace Studies, 2(1), 2009.


Zaman, Muhammad Qasim, ‘The Ulama in Contemporary Islam: Custodians of Change.’
Chapter 11

Prevention of Radicalization in Western Muslim Diasporas

Nina Käsehage

This chapter opens with a brief definition of key terms such as “Muslim diasporas,” “prevention of violent extremism” (PVE), “countering violent extremism” (CVE) and discusses the role of Islamophobia in radicalization and its impacts on the prevention of radicalization. The size of the Muslim population in each of the selected five Western countries and the appearance of jihadist, left- and right-wing-groups, as well as the number of attacks resulting from these milieus are briefly discussed at the beginning of the country reports. The main body of this chapter discusses academic, governmental, and civil society approaches to PVE/CVE. For each country, some PVE examples are presented which might be helpful to policymakers and practitioners. A literature review regarding PVE/CVE approaches in each country seeks to provide an overview of the academic state of the art concerning the prevention of radicalization. Finally, a number of recommendations with regard to future PVE initiatives are provided, based on the author’s field research in Salafi milieus in various European countries.¹

Keywords: countering violent extremism (CVE), countering violent extremism policy and practice, extremism, government and civil society responses, Muslim communities, Muslim diasporas, prevention, preventing violent extremism (PVE), PVE recommendations, radicalization, religious extremism, Salafism, terrorism
This chapter seeks to describe the state of research on the prevention of radicalization in Western Muslim diasporas. For this purpose, the following countries were selected: Belgium, Denmark, France, Germany, and UK.2

First, the main terms used in the title of this chapter will be discussed briefly, focusing on religious extremism.3 The understanding of “radicalization” and “prevention” is not uniform in Western societies. That discussion leads to the question of the definition of Muslim diasporas - a composite term that might also vary, depending on the point of view: Is it used to describe an insider Muslim perspective, or a situation as perceived by Western societies hosting Muslim immigrants?

A person’s perception of the term “Muslim diasporas” might itself lead to grievances. This may make some individuals more susceptible to radicalization, e.g. when Muslims see themselves as citizens of Western countries they are living in (in particular if they were born there or are part of the second or third generation), but are still perceived and treated like “foreigners.”

Secondly, a number of research approaches related to the prevention of radicalization and to current debates within this field will be discussed as they relate to the five Western countries considered in this chapter. In this context, it is important to state that only a selection of the literature and only some of the initiatives related to the prevention of radicalization can be described here.

By discussing the efforts of national governments and local communities, as well as the findings of researchers, some helpful insights on the methods and mechanisms of radicalization prevention can be brought to the attention of policymakers, counterterrorism professionals, civil society stakeholders and others directly confronted with the phenomenon of radicalization. A few examples of good practices and approaches are also presented. Following the conclusions, recommendations are made, based on the author’s personal field-research.

Prevention, Radicalization and Western Muslim Diasporas - Can a Single Definition Fit all Countries?

In order to prevent radicalization in Western Muslim diasporas, it is important to understand the mechanisms and the multiple drivers behind radicalization, in particular those related to religious radicalization. According to Vidino, radicalization is “a highly individualized process determined by the complex interaction of various personal and structural factors.”4 Lambert and Wiktowicz argue that religious fundamentalists are cognitive extremists of whom just a minority are likely to turn to militant jihad.5 Ravn, Coolsaet, and Sauer underline a very important aspect within this debate when they note that “despite a lack of a scholarly consensus on how to understand radicalization, a set of preconceived ideas about the phenomenon is taken for granted in the public discourse.”6 Different understandings of radicalization become significant in the context of selecting best approaches to strengthen prevention efforts. If the starting points towards a certain phenomenon differ, efforts to achieve common aims are likely to run into difficulties. Due to this, we should free ourselves from the idea that a mono-causal explanation for radicalization exists which applies to every “radical.” Living in a complex world requires an ability to react in a flexible way. When it comes to prevention, what works in a non-Muslim context might differ in a Muslim-majority country context.7

Some terms are “loaded” and if they contain overt or covert elements of discrimination, they are unlikely to open doors to the very group of people which need to be brought back to a peaceful path.8 A term like “Muslim diaspora” can be a neutral description of a religious minority, but can also be understood as excluding a whole segment of a minority group from society, even those persons who were born in the “West.” This is not the place to discuss the
“us” versus “them” implications of such perceptions, but it is something we have to keep in mind when discussing prevention of radicalization.

In this chapter, various approaches in the field of the prevention of radicalization are discussed. The existing literature generally distinguishes between preventing violent extremism (PVE) and countering violent extremism (CVE). According to Daniel Koehler:

“PVE programs can be defined as programs designed to prevent recruitment and radicalisation into violent extremism leading to terrorist actions. These programs can address individuals or groups not at risk of violent radicalisation (primary or general prevention, resilience building), or those already considered to be at risk or in the early stages of a violent radicalisation process (secondary or specific prevention, early intervention). Deradicalisation programs are usually not counted among PVE efforts, but rather belong to CVE (countering violent extremism) methods.”

This chapter focuses mainly on PVE approaches that are primarily understood as prevention of radicalization of individuals and groups of people to violent extremism and terrorism. Nevertheless, referring to Koehler’s approach - deradicalization as a form of CVE - can be seen as being closely linked to PVE approaches.

Although several causes for radicalization to violence exist that do not relate to religion, but to other factors such as economic inequality, religion is often seen as the most important driver for the current wave of terrorism – more so in the public debate than in scholarly publications. Cavanaugh calls this mechanism: the “othering” of religion, writing:

“The myth of religious violence helps to construct and marginalize a religious Other, prone to fanaticism, to contrast with the rational, peace-making, secular subject. This myth can be and is used in domestic politics to legitimate the marginalization of certain types of practices and groups labelled religious, while underwriting the nation-state’s monopoly on its citizens’ willingness to sacrifice and kill. In foreign policy, the myth of religious violence serves to cast non-secular social orders, especially Muslim societies, in the role of villain.”

The effect of the “othering” of religion in largely secular states, e.g., for purposes related to domestic political debates, can be seen as a key for some young Muslims in western diasporas to embrace radical religious thoughts. Although some of these vulnerable Muslims were initially not familiar with fundamentalist religious interpretations of Islam, everyday discrimination due, for instance, to their wearing specific clothes such as the hijab or the jellabiya, and media reports portraying “the” Islam as a violent religion, can be seen as partially responsible for the radicalization of some young Muslims across Europe, with radicalization (also) being a form of protest.

The European Commission against Racism and Intolerance (ECRI) as well as the Council of Europe in the “Annual Report for 2018” noted:

“Islamophobia is still prevalent … In public discourse, Islam and Muslims continue to be associated with radicalization, violence and terrorism. There is, generally, only very little positive media coverage of Muslim communities in Europe. Islamophobic hatred is often spread via the Internet. Anti-Muslim sentiments are also regularly manifested in petitions and protest rallies against the construction of mosques. In many member states, a dangerous ‘normalisation’ of Islamophobic prejudice can be observed.”
This “normalization of Islamophobic prejudices” and its particular impact on black Muslims (which was addressed by ECRI as well), can be seen as a major push factor for the radicalization of some young Muslims. While a recent report on Islamophobia correctly noted that “Muslims are … the people who suffer the most from terrorism emanating from radicals in the Muslim world as the vast majority of terrorist attacks occur in Muslim-majority countries,” the Western public tend to perceive attacks within the West as more cruel than the ones which occur within Muslim-majority countries.

In addition to experiences of everyday discrimination against Muslims in Western countries - which is partly due to how some may negatively perceive their style of clothing and their public expressions of religiosity - another aspect affects the lives of (young) Muslims in the “West”: “a new kind of terror rooted in anti-Muslim racism and white supremacist ideology.”

By looking at Western Muslim diasporas, one also ought to look at the subjectivity of some researchers regarding the issue of Islamophobia. Very often, their individual understanding of radicalization and its potential prevention is a result of their own positioning vis-à-vis the religion of Islam and its believers. A good example in this context is the development of Islamophobic incidents within Europe. Some researchers, e.g., Günther Jikeli, try to assess various forms of discrimination such as “racist or xenophobic, anti-Muslim and anti-Semitic acts” on the basis of their numbers, not on account of the level of discrimination. That this argument could be seen as a discriminatory position of the researcher towards a specific group itself, seems to be excluded from his conclusion:

“Anti-Muslim acts do exist and might be on the rise, but they have not supplemented racist manifestations in Europe in recent years, and they stay below the number of anti-Semitic acts. […] However, there is a growing sense of victimhood on the basis of Islamic belief. Debates on Islamic fundamentalism and increased anti-terror measures are often viewed by Muslims as anti-Muslim bias.”

According to Jikeli, Muslims and Islamic organizations themselves are held responsible for “recent debates about a rise of ‘Islamophobia’ (…) that try to prohibit critical debates about some interpretations of Islam, blur[ring] the lines between such criticism and hatred of Muslims.” Although this argumentation might hold true for some Islamic organizations, it is widely used as a narrative to suppress critics of discrimination against Muslims, especially among right-wing political parties such as the Alternative for Germany (AfD), The Republicans (Les Républicains) in France, the Progress Party in Norway, and the Liberal Party of Denmark (Venstre).

In an article titled “Discrimination against Muslims and Antisemitic Views among Young Muslims in Europe,” Günther Jikeli presented a table, combining data from two surveys, one from the Pew Global Attitudes Project “Unfavorable Views of Jews and Muslims on the Increase in Europe” from 2008, and the second from the Pew Global Attitudes Project “Muslims and Islam: Key Findings in the U.S. and around the World” from 2017. The table, titled “Unfavorable Views of Muslims in France, Germany, and the United Kingdom,” presented data on these countries from 2004, 2005, 2006, 2008 and 2016 in order to highlight that:

“Negative views of Muslims and Islam are prevalent, but contrary to common belief, such views have not increased since 2004, despite the wave of terror attacks in the name of Islam. In spring 2016, 29 percent of the population in Germany (46 percent in 2004), 28 percent of the population in the United
However, these “findings” stand in stark contrast to statistics presented in the “Islamophobia Report 2018,” which is based on surveys held in 34 European countries:

“The Collective Against Islamophobia in France (Collectif contre l’islamophobie en France or CCIF) recorded 676 Islamophobic incidents in 2018 against 446 in 2017 (increase of 52%). In the UK, the upward trend in Islamophobic incidents continued in 2017-18 (the typical census period for official government data), with the number of cases recorded in official statistics rising by 17% and religion-specific cases by a staggering 40% (double the figure of 2015/16).”

Most of the Islamophobic incidents, e.g., in France, were directed against women. In Europe as well as in other “Western” countries, an increased number of attacks on Muslim women who wear a veil-variant has been registered. This means that Islamophobia contains a gender-specific discrimination towards female believers. It might be the result of the idea that women are (often) responsible for the “education” of the next generation. With regard to Islamophobic attacks, for instance in Germany, Younes stated that they

“Have to be seen in conjunction with attacks on refugees, their asylum homes as well as NGOs in the services of refugees and their problems. Until the end of 2018, around 1,775 attacks on refugees took place, with around 329 adults and 15 children hurt. Overall, we observe a decline in the reporting and/or registration of physical attacks compared to the previous years.”

This finding underlines the fact that Islamophobia can be both a source of Muslim radicalization and violence, and a cause of reciprocal radicalization by right wing militants. Furthermore, the conflicting outcomes of surveys regarding Muslims, Islam, and the development of Islamophobia can be seen as a result of the use of different terminologies regarding the same phenomenon. This mechanism could easily be extended to the discussion of the prevention of radicalization. Therefore, it is important to keep this heterodox approach in mind, in terms of the religion of Islam, its believers, and the debate about the prevention of radicalization in Western Muslim diasporas. It might become more visible in the following literature review and in the case studies of prevention approaches in the five Western countries that are discussed in this chapter. In terms of increasing Islamophobia, rising right-wing politics within these Western countries and a fear of Muslim immigrants, who are often blamed for being potential terrorists, the term “Radicalization” itself is also often stereotyped.

With regard to the possible “amount of growth in Europe’s Muslim population” within the framework of “future migration” in 27 European countries, the UK, Norway and Switzerland, the US-based Pew Research Center estimated a growth from 4.6 percent of the whole population in 2015 up to 14 percent (in a high migration scenario), 11.2 percent (in a medium migration scenario) and 7.4 percent (in a zero-migration scenario) in 2050.

The estimated “World’s Muslim Population” is likely to increase from 5.9 per cent Muslims in Europe in 2010 to 10.2 percent Muslims in 2050 and from 1 per cent Muslims in North America in 2010 to 2.4 per cent Muslims in 2050 in North America. Such projections might serve as an explanation for an increase of negative right-wing sentiments regarding the presence of Muslims in the West.

In addition, it is important to note that next to Islamophobia research, investigations about the “mediating role of acculturation in the relationship between perceived threats and support
of violence” among Muslim communities exist. In applying the Integrated Threat Theory (ITT), it is evident that perceived threats as well as hostility towards a specific group, such as members of Western Muslim diasporas, could construct negativity and hostility towards an out-group as a result of discrimination against the former.

For these reasons, the chapter title “Prevention of Radicalization in Muslim Western Diasporas” contains various (individual) implicit assumptions and challenges regarding the prevention of religious related radicalization itself.

**Review of Selected Governmental Approaches and Literature about Radicalization and the Prevention of Radicalization in Western Muslim Diasporas**

Before turning to national responses, it is useful to recall some key developments on the international (UN) and regional (EU) levels.

In 2015, the UN’s “Plan of Action to Prevent Violent Extremism” (PVE Plan) was presented to the General Assembly. The PVE concept differs from the CVE approach as it focuses more on root causes leading to violent extremism. In order to strengthen community resilience, the plan includes various recommendations for the prevention of terrorism and violent extremism on the international as well as on the local level. In 2017, the UN’s Educational, Scientific and Cultural Organization (UNESCO) released the publication “Preventing Violent Extremism through Education: A Guide for Policy-makers.”

According to the release “The Council Conclusions on EU External Action on Preventing and Countering Terrorism and Violent Extremism” of 16 June 2020, the European Council “recalls that security at home depends on peace and stability beyond the EU’s borders” and a “further strengthening of the EU’s external counterterrorism engagement and action in the priority geographic and thematic fields.” Threats related to terrorism, a focus on further geographical EU investments and priority areas for action such as the Western Balkans, the Middle East and North Africa (MENA) region, the Sahel region, and the Horn of Africa, as well as the importance of improved international cooperation are issues emphasized in the European Council report. In addition, the report calls for support of the priority partner countries which are the most impacted by the “returnees” phenomenon, “in order to help them bring perpetrators to justice, address radicalization leading to violent extremism and terrorism in prisons, and support rehabilitation and reintegration activities, including of family members, as well as specialised services for returning children.”

The Council underlines the need for compliance to all CVE measures with EU core values such as the rule of law in agreement with international law (international human rights law, humanitarian law and international refugee law).

The report highlights the need for a “whole-of-society” approach to prevent and counter violent extremism, and also notes that deradicalization efforts need to address the essential conditions beneficial to terrorism and radicalization; the continuous care for vulnerable groups such as children and women; a gender approach with regard to female empowerment and the support of their resilience toward radicalization, as well as the strengthening of contact to civil society, youth, human rights defenders and victims of terrorism. It notes that “involving civil society organisations in countering terrorism and preventing violent extremism remains of utmost importance for a successful approach. It is also important to continue addressing the spread of violent extremist narratives and to further promote interfaith and intercultural dialogue.”

Therefore, in the field of CVE and PVE, a continuing support of enhanced EU external actions, e.g. on online platforms - increasingly important areas for violent extremist Islamist ideology of Da’esh and al-Qaeda, has been suggested. It is also noted that foreign terrorist fighters should be brought to justice and their movements be prevented.
The report further noted that one of the impacts of the COVID-19 pandemic might be its “potential influence on terrorist activities as well as on the prevention and countering of terrorism...”46 In order to prevent radicalization leading to violent extremism and terrorism, the Council suggested “the development of assistance programming, where appropriate, as well as country-specific and regional strategies”47 and a multi-stakeholder approach whereby “industry works together with EU and partner-country governments as well as academia and civil society in preventing and countering terrorism.”48

UN Secretary-General António Guterres noted that “terrorism is fundamentally the denial and destruction of human rights and the fight against terrorism will never succeed by perpetuating the same denial and destruction.”49 Member states of the UN have reacted in various ways to the common problem of radicalization and the resulting “home-grown” terrorism emerging within Muslim diasporas in their societies.

In the following section, developments in five Western countries will be sketched briefly. These lead to various prevention-oriented recommendations. New directions and challenges in the field of prevention of radicalization are addressed, illustrated by references to various national, regional, or subject-specific experiences.

Belgium

In Belgium, 7.6 percent of the total population were Muslims in 2016.50 The projected percent of Muslims of the total population in Belgium in the year 2050 is estimated at 11.1 percent (estimate with zero immigration), 15.1 percent (estimate with medium immigration) and 18.2 percent (estimate with high immigration).51 The Pew Research Center’s survey regarding the destination of migrants to Europe ranked Belgium with 230,000 migrants (57 percent of whom are Muslims) in the position. With regard to the number of Muslim refugees, Belgium is seventh in Europe, with 40,000 Muslim refugees.52

Molenbeek, a suburb of Brussels, became internationally known as a hot-spot for jihadist radicalization since the attacks of November 2015 in Paris and March 2016 in Brussels, committed by young jihadists from Molenbeek claiming allegiance to ISIS.53 The militant jihadist group Sharia4Belgium is the main violent extremist group; it inspired other groups to radicalize, by providing a jihadist infrastructure.54 Many of the foreign fighters from Western European countries came from Belgium55 and 86 per cent of them were already “known to authorities for offences such as robberies, theft or drug dealing.”56

In order to address this rising trend, the Belgian government initiated PVE programs in 2013 and established a taskforce to develop a national counterterrorism and counterextremism strategy in 2015.57 In this context, a 12-point action plan against terrorism was created. It included the creation of a new National Security Council, chaired by the Prime Minister, and also involves the domestic deployment of the military whenever the threat level is raised significantly, the development of new deradicalization programs in prisons, and also the strengthening of existing legal frameworks to deal with the phenomenon of foreign fighters.58 Furthermore, various CVE initiatives for ten cities in Belgium that faced specific radicalization threats came into existence; these also included PVE approaches, e.g. one focusing on extremist messaging on the internet.59 According to Pauwels et al., online exposure to extremist messages can promote political violence.60

According to an examination of the Belgian State Security Service from 2017, “nearly 5 percent of all prisoners in Belgium – 450 prisoners in all – pose a radicalization threat.”61 The report found that European cells “partially fund themselves through crime, such as petty theft, shoplifting, and extortion. Some jihadist preachers have reportedly legitimised such offences if used to finance jihad.”62 Such findings suggested that a stronger PVE approach focusing on prisons and probation cases was called for.
Apart from the jihadists, groups as well as individuals of the anarchist and left-wing extremist milieu such as some of the participants of the *gilets jaunes* (yellow vests) movement, pose a threat to public order in Belgium due to their sometimes violent demonstrations. The Belgian far-right is most visible in the Flemish party *Vlaams Blok* (Flemish Bloc). It was forced to disband in 2004 as a consequence of its discriminatory statements against immigrants. After that, many members of the Vlaams Blok regrouped under the umbrella of another less extreme party, *Vlaams Belang* (Flemish Interest). Wallonia, the French speaking part of Belgium - traditionally a strong base of the socialist party - has witnessed the rise of the *Parti Populaire* (People’s Party). Its leader Mischael Modrikamen aligned with various leaders of foreign nationalist parties (e.g., Geert Wilders in the Netherlands and Nigel Farage in the UK) who are known for their Islamophobic attitude. Some right-wing extremist groups organized anti-Muslim and anti-migrant demonstrations.

Although no terrorist attacks took place in Belgium during 2019, a number of attacks in the planning stages and instances of individuals providing material support to terrorists have been registered but were prevented, partly thanks to the monitoring of over 200 radical individuals. A total of 89 convictions and acquittals related to jihadist terrorism have been pronounced by Belgian courts in 2019. In addition to 11 arrests for jihadist terrorism, 86 persons have been arrested for non-specified types of terrorism while two persons were apprehended for ethno-nationalist and separatist activities. In addition, “one jihadist-terrorism affiliated attack was foiled.”

**Governmental PVE Strategies**

With regard to the prevention of radicalization, various communities as well as the Belgian government prepared information instruments for schools. One of these is the Prevention Pyramid, a five-level instrument that addresses radicalization at different stages. It is used at the Royal Atheneum of Antwerp, but also by other stakeholders.

The project, Identity and Communication - Based on the Logical Levels of Bateson, is another training program for teachers addressing identity formation. Due to the increased impact of Sharia4Belgium within schools, it enables pupils to comprehend religion as a system of beliefs that shape individual identities. The courses are based on a four-level training for teachers who face students at risk of radicalization in their classrooms. They are trained to use neuro-linguistic programming (NLP) techniques to counter negative self-images of pupils. NLP is also said to develop their confidence in order to make them more resilient against religion-related radicalization attempts and imparts them with a feeling that their future is not pre-determined by religious laws.

The Athena-Syntax project is an educational project of the European-wide Radicalization Awareness Network (RAN). It provides an interdisciplinary structure for students and teachers, allowing them to exchange views in a horizontal dialogue, focusing on core human values. Artwork is developed under the guidance of professional artists who work with students outside the school. This gives young people a chance to express their emotions, fears, and questions through art so that they channel their anger and frustrations in positive ways.

**BOUNCE** is a training and awareness-raising tool for young individuals at risk due to their social environment. It provides preventive measures against violent radicalization. It is a program of the European Commission Prevention of and Fight Against Crime (ISEC). Strengthen Resilience against Violent Radicalisation (STRESAVIORA). BOUNCE Young has been developed for young people to strengthen their resilience. It also serves parents of vulnerable children as well as frontline workers. It provides recommendations, insights, and exercises for adults in order to allow them to better understand the social environments of their kids. BOUNCE Up is a train-the-trainer tool for frontline workers.
Selected Belgian Literature on Radicalization and the Prevention of Radicalization

One study with the title “Exploring the discrimination-radicalization nexus: empirical evidence from youth and young adults in Belgium,” observed a potential link between the perceived discrimination and the support for violent extremism among youth and young adults in Belgium. One of this study’s findings is that “over half of individuals who identified as Muslim (55.6%) reported some kind of discrimination, 19.5% [of the] Muslim[s] were also more likely to report experiencing discrimination in the justice system.” Such perceived discrimination can sometimes act as trigger for radicalization. The theme of prevention through integration of young adults with an immigration background is therefore prominent within the Belgian literature on radicalization and in recommendations for its prevention. The study “Loss of Identity, Radicalization, and Terrorism. Case Studies in France and Belgium” identified the lack of a (national) identity and a need for belonging as major causes of radicalization leading to an increased interest in terrorism in Belgium as well as in France.

Other researchers identify psychosocial factors among specific groups, e.g., refugees, within Belgium as possible push factors for radicalization. The need for family support for vulnerable young adults emerged in a study by Gielen as key for the prevention of radicalization in Belgium. There are many governmental and non-governmental efforts to prevent radicalization in Belgium. Three of these stand out:

1. Theological Pilot Project: theological approach to Islamic radicalism (Theologisch pilot project: theologische aanpak van islamitisch radicalisme): This theological pilot project developed by imams and Islam-experts in Flanders tries to prevent radicalization by drawing on religious knowledge and is linked to the Platform of Flemish Imams and Muslim Experts (Vlaams Platform Radicaliserings and Platform van Vlaamse Imams en Moslimdeskundigen, or PVIM).

2. KLASSE: This initiative aims to impart Islamic knowledge to pupils by recognized religious authorities such as Imam Khalid ben Haddou. It seeks to target radicalization as well as the development of Islamophobia in Belgian schools.

3. S.A.V.E. (Society Against Violent Extremism): This is an initiative of parents of (former) radical Islamic militants. It aims to impart awareness about radicalization in society from the perspective of affected families. It tries to prevent further radicalization by highlighting the need for psycho-social support of vulnerable persons and their families. It also seeks to strengthen intercultural dialogue and create action plans (Le Tableau Des Actions) for the prevention of radicalization through education and mutual assistance.

The main feature of Belgium’s prevention approach is its holistic strategy, involving a support network from the local educational sector and from welfare organizations, Flemish employment services as well as job centres, schools, health services, police and justice. These are all linked to a Central Help Desk (CHP) that provides support to young individuals at risk at short notice (within one week). The idea of this prevention network is to avoid a pupil’s expulsion from school. It enables vulnerable individuals to access the labour market or higher-education in order to strengthen their resistance against recruitment by radical organizations. The city of Antwerp developed an education policy that is applicable to all schools in this area; it maintains cooperation with prevention of radicalization services in 26 European countries.

Given Belgium’s multilingualism, namely French, Flemish, German, English and Arabic (in some cases), the exchange and the cooperation between jihadist actors and networks is much more pronounced than in most other European countries. This could also be noticed from the connections between the Paris-attackers and the Brussels-attackers of the year 2016.
Denmark

In Denmark, 5.4 per cent of the total population were Muslims in the year 2016.\textsuperscript{90} The projected percentage of Muslims of the total population in Denmark in the year 2050 is estimated at 7.6 per cent (estimate with zero migration), 11.9 per cent (estimate with medium migration) and 16 per cent (estimate with high migration).\textsuperscript{91}

In 2019, the Danish authorities noted that Islamist and jihadist groups in Iraq and Syria remained the primary recipients of terrorist financing from Denmark-based individuals with ties to Sunni Muslim networks. The amount of the transfers decreased due to the reduced opportunities for transferring funds to the (declining) ISIS and because of the small number of remaining Danish citizens within the zones of armed conflict.\textsuperscript{92}

With regard to prisons, Europol noted that “Denmark is concerned that radicalized inmates in contact with people from organized crime circles may pose an increasing risk of jihadists gaining access to weapons.”\textsuperscript{93} Convictions and acquittals for terrorist offences in 2019 in Denmark were related exclusively to jihads. There have been 21 arrests for jihadist terrorism and four convictions and acquittals for jihadist terrorism, while two jihadist attacks were foiled.\textsuperscript{94} In December 2019, arrests were carried out in several locations in Denmark. Seven persons were charged with planning and preparing two separate jihadist attacks in Denmark or another European country.\textsuperscript{95} With regard to the left-wing extremist milieu in Denmark, collaboration between Norwegian and Swedish groups and other European like-minded groups was observed in 2019.\textsuperscript{96} Danish right-wing extremist movements increased their ties “to like-minded individuals abroad, including on virtual platforms.”\textsuperscript{97} Several anti-Jewish acts e.g., in November 2019, when Danish right-wing extremists “committed acts of gross vandalism and desecration of Jewish symbols and graves,” have been observed.\textsuperscript{98}

\textit{Governmental PVE Strategies}

Following several terrorist incidents, e.g. an attack on a synagogue in Copenhagen as well as the “cartoon crisis,” Denmark has strengthened its PVE efforts by means of an Administration of Justice Act. It postulated a multi-sectional collaboration between agencies, organizations, and institutions\textsuperscript{99} based on local and regional best practice examples.\textsuperscript{100} The Danish P/CVE approach goes back to the year 2009 and has become known as the Aarhus Model.\textsuperscript{101} It involves a cooperation of state as well as municipal structures and focuses mainly on vulnerable individuals,\textsuperscript{102} paying special attention to forms of peer monitoring, and educational and psychological support, which is likely to have a positive impact on individuals in terms of providing them with a clearer understanding of their identity and instilling in them a sense of belonging.\textsuperscript{103} By tackling intolerance, frustration, and other possible push-factors towards radicalization, this approach amounts to an active form of community-based prevention.\textsuperscript{104} The plan includes:

“22 initiatives that would strengthen democracy and provide alternatives to extremism. This would revolve around counter-terrorism, efforts against gangs and youth crime, international co-operation on peace, development and democracy, efforts against discrimination and intolerance, education, jobs and opportunities for all, and integration and intercultural dialogue.”\textsuperscript{105}

The Danish PVE strategy is built on a partnership of major actors in the field of the prevention of radicalization and focuses on three aspects:

1. A prevention and exit strategy;
2. The prosecution of radicalized persons;
3. The prevention and countering of threats to national security.\textsuperscript{106}
The Aarhus Model became a conceptual role model for other Western countries with regard to early prevention and exit processes. It aims “to stop or redirect the process of violent radicalisation” and is characterized by the reintegration of radicals into society while downplaying “the ideologies as a cause for recruitment into extremist organisations.”

Based on a cooperation of the Danish Security and Intelligence Service (Politiets Efterretningsstjeneste, PET), the Department of Psychology and Behavioral Sciences, and various experts from academia, social services, and ministries, the interdisciplinary approach unifies methods from personality psychology, social psychology, societal psychology, social science, and the humanities. The Aarhus Model is based on six steps:

- Step 1: Information, e.g., from the social environment of an affected individual, regarding his/her potential extremist attitude, is forwarded to the “Info-house” (staffed by the East Jutland Police);
- Step 2: Further information is gathered by the police to assess the situation in detail;
- Step 3: If the results of these investigations lead to the decision that the individual is showing signs of “pre-radicalization,” an interdisciplinary workshop is organized that provides support or counselling;
- Step 4: In cases of “false positives” or “youth rebellion” signs, social services and other relevant measures will be recommended.
- Step 5: If risk factors of violent radicalization are identified, the Information House will start an assessment and stay in contact with the affected person and involve members from the social environment;
- Step 6: Mentors with broad expertise in the field of (prevention of) radicalization will provide social and legal alternatives to resolve personal conflicts.

In 2013 an exit program was added to the Aarhus Model in order to “de-radicalise returning foreign fighters by reintegration efforts that help transition the individual back into society and daily life.” Based on the specific needs of the individual returnee, a task force recommends the kind of assistance which should be offered to the returnee and to his/her social network (e.g. family, friends, school) in order to provide the best possible way for his/her reintegration. On the basis of a written exit-process agreement between the returnee and those responsible for the exit program, specific help suggestions are provided, e.g., with regard to therapy, medical care, employment and accommodation. It is important to note that the exit program includes an exception clause regarding its target group: it only accepts foreign fighters who did not commit any criminal acts and are deemed to pose no security risk to Danish society. This seems to be a problem, because it is widely known that most of the foreign terrorist fighters (FTFs) already committed (mostly minor) crimes, before they went abroad. In addition, their participation in ISIS (which might have included fighting against others and probably also killing people) is also seen as a crime. Although the position of the “exit program” regarding possible misuse of the Aarhus Model by some returnees is clear, the practical application is not.

In 2014, the Danish government launched its Prevention of Radicalisation and Extremism: Action Plan, based on a dozen initiatives, with a focus on increased involvement of local authorities. It focuses on “pre-radicals” who are 18 years or over and involves strategic partnerships with local authorities, skills-enhancement programs, and additional intervention steps.

An additional focus has been on the development of new P/CVE tools, including:

1. methods for prevention and interventions at an early stage (initiative 4);
2. increased online presence (initiative 5);
3. measures regarding recruitment to terrorist groups to participate in armed conflict abroad (initiative 6);
4. improved exit programs (initiative 7); and
5. closer international partnerships (initiatives 8 and 9).\textsuperscript{116}

Furthermore, it recommended a larger degree of civil society collaboration with local authorities (initiative 10) as well as enhanced participation of parents of vulnerable and/or radicalized youth (initiative 11).

In 2016, a National Action Plan “Preventing and Countering Extremism and Radicalisation,” was made public.\textsuperscript{117} It covers, inter alia, better coordination of evidence-based prevention approaches, issues related to P/CVE online and prison approaches, greater involvement of local communities and municipalities, as well as strengthening of international cooperation.\textsuperscript{118}

Against the background of concerns regarding detained ISIS fighters who could escape SDF detention as Turkish forces entered northeast Syria, Denmark’s parliament passed in October 2019 a bill concerning the revocation of Danish citizenship in the case of dual citizenship of FTFs.\textsuperscript{119} The new law, which allows citizenship revocation without a trial, states that anyone acting in a manner seriously prejudicial to Denmark’s vital interests may have his or her Danish citizenship revoked, unless the person would be rendered stateless.

\textit{Selected Danish Literature on Radicalization and the Prevention of Radicalization}

Tammikkoa examined the political challenges of community-level PVE practices in Copenhagen and Aarhus. He found, inter alia, that “regarding practices related to Preventing Violent Extremism (PVE): a community-level dialogue was discontinued with an extremist milieu in Copenhagen due to the specific worldview but allowed to continue in a similar situation in Aarhus.”\textsuperscript{120} Furthermore, confusion regarding the new concept of PVE and political issues, the decision-making structures and the development of “coherent PVE practices with a solid understanding of PVE goals on a political level” were seen as major challenges in Denmark.\textsuperscript{121}

Bertelsen examined the “Danish Preventive Measures and De-radicalisation Strategies” of the Aarhus Model with regard to its beginning and evolution in view of its exit program. Her article provides important insights on the development of this – in the beginning unique – Danish prevention concept.\textsuperscript{122}

Gielen’s articles “Anti-radicalization in Belgium, Denmark and Germany” \textit{(Antiradicaliserin in België, Denemarken en Duitsland)}\textsuperscript{123} and “Syria fighters: Rather support families than take their passport” \textit{(Syrië-strijders: liever families ondersteunen dan paspoort afnemen)}\textsuperscript{124} are highly recommended in terms of providing a deeper understanding of the motives of FTFs and their family backgrounds in Denmark, Belgium and Germany.\textsuperscript{125} Gielen’s work on exit programmes for female jihadists,\textsuperscript{126} her study on the assessment of CVE initiatives,\textsuperscript{127} and her recently published doctoral thesis on the evaluation of CVE deal with various challenges linked to the Danish (re-) integration process of different types of jihadists against the background of practicability and usability of existing P/CVE approaches.\textsuperscript{128}

Another commendable report is Koehler’s examination of the concept of family counselling, de-radicalization, and counterterrorism, involving a comparison between Danish and German programs.\textsuperscript{129} It addresses the need for, and examines the effectiveness of, family counselling regarding (pre-)radicalized individuals at a time when Germany was not aware of its importance, offering several insights based on the Danish model.

There are many other governmental and non-governmental efforts to prevent radicalization in Denmark. Three of these stand out:

1. **The Centre for Prevention of Extremism**: This governmental Centre for Prevention of Extremism brings together multiple stakeholders from the whole of Denmark and offers intervention tools for helping individuals who are entangled in extremist circles,
as well as providing preventive measures for individuals at risk, while also offering
support for children and young adults.130

2. Centre of Prevention: PET also houses a Centre of Prevention. It coordinates crime
prevention networks (SSP - schools, social services and police), PSP (psychiatric
sector, social service, and police), and KSP (Danish Prison Service, social service,
and police) within its structure. The PET Centre of Prevention offers support for those
wanting to leave militant extremism (EXIT) as well as for individuals and groups at
risk of becoming radicalized (capacity building) while also addressing certain social
preconditions in its outreach activities.131

3. Unit for the Prevention of Extremism and Radicalization (Forebyggelse af
ekstremisme og radikalisering, VINK): VINK is a prevention initiative of the
municipality of Copenhagen that offers general information regarding the prevention
of radicalization for affected families and the public at large. It also offers advice and
counselling by professionals, and provides coaching and mentoring for families.132

While the success of the Aarhus Model has been widely acknowledged, some critical voices
focused on the selection of employees in CVE environments and CVE policies in general.133

Johansen points out that “the Danish case shows, [that] the detection and categorization of the
concept of radicalization is not a straightforward process at the front line of the state.”134 The
responsibility of naming and defining the phenomenon of radicalization is tied to the particular
role of the “expert” within the bureaucratic system. However, these “experts” may have been
more or less randomly selected for the task.135 The ever present “terror threat” could lead into
an endless “risk assessment that categorizes risk [on the basis of] second-hand information” to
“categorical suspicion.”136 According to Johansen, “it is this balancing act between the politics
of anxiety and the potential for public moral outrage that I regard as one of the basic elements
current bureaucratic CVE practices in Denmark.”137

Similar to the strategy of the British government, the approach towards the question of
repatriation of former Danish foreign fighters or the revocation of their Danish citizenship in
terms of a dual-national citizenship is questionable with regard to its effectiveness in terms of
the prevention of radicalization. On the one hand, it could be seen as a deterrent for others,
telling them not to follow the path of violent extremism without risking the loss of links to their
places of origin forever. On the other hand, those defectors who only possess one citizenship – the Danish citizenship - cannot be stripped of it. That would indicate discrimination against
some former FTFs of foreign heritage. In this regard, the results of hardliner policies have not
been assessed. It is still possible that they could be counter-productive and lead to solidarization
effects within the Islamist milieu.

France

In France, 8.8 per cent of the total population were Muslims in 2016.138 The projected
percentage of Muslims of the total population in France in the year 2050 is estimated at 12.7
per cent (estimate with zero immigration), 17.4 per cent (estimate with medium immigration)
18 per cent (estimate with high immigration).139 The Pew Research Center’s survey regarding
the destination of migrants to Europe ranked France at third place with 530,000 Muslim
migrants and ranked sixth in Europe with 50,000 Muslim refugees.140

In 2019, 202 persons were arrested based on charges related to jihadist terrorism, seven
individuals had been arrested for right-wing extremism and 13 persons were detained for ethno-
nationalist and separatist terrorism in France.141 Four jihadist attacks, including those on March
25, April 26, and September 23, were foiled in 2019.142 Three jihadist attacks took place in
France, including one in May 2019 in Lyon in a pedestrian zone by a student, and another in
October in Paris by an IT specialist working for a police intelligence unit in Paris.143
French courts issued multiple convictions (105) as well as several acquittals related to jihadist terrorism in 2019. Between 2018 and 2019, four attacks within French prisons, including one at the Condé-sur-Sarthe prison in March 2019, were foiled. There have also been several female Islamist terrorists imprisoned in France in recent years.

The Children’s Court of Paris issued a sentence against a French-Algerian minor charged with participation in a criminal conspiracy involving the preparation of a terrorist act in the name of ISIS against police officers. In another case, the Children’s Court of Nancy sentenced three French minor offenders from Belfort for preparing a terrorist act. The close connection between Belgian, Dutch, and French jihadist networks is still an important source of concern. According to Europol:

“In the Netherlands, the District Court of Rotterdam heard the cases of several defendants investigated in relation to the discovery of a large amount of ammunition. The defendants were suspected of having been involved in the supply of (part of) the ammunition found in an apartment in Argenteuil (France) in March 2016 that was used by a transnational network of jihadists from Belgium, the Netherlands and France.”

Right-wing extremism in France is characterized by various features “such as structured right-wing extremist movements,” e.g., the neo-fascist Troisième Voie (Third Path) and the monarchist Action Française (French Action). These “have lost influence following self-dissolutions in 2014, in an attempt to avoid formal bans following the death of a left-wing activist during an attack.” In addition, the French white supremacist movement Suavelos provides an internet platform for white supremacists, whose messages have been exposed and faced deletion on major platforms like Facebook and YouTube in the wake of the Christchurch attacks.

Non-structured right-wing extremists in France try to distinguish “original” French natives from those with a Muslim heritage, e.g. by propagating the Great Replacement conspiracy theory, claiming that Muslims plan to replace the original Europeans and “overrun” Western countries.

In addition to militant movements, the National Front (Front Nationale) and its “neo-conservative” politics have still influence on many French (voters), using Muslim immigration and refugee politics as well as Islamophobia for gaining electoral support. Two attacks on mosques in Brest and Bayonne took place in 2019. The latter incident was reported as being the work of a neo-populist fringe group from the right-wing extremist scene. With regard to left-wing extremism in France, several militants engaged in violent acts towards public institutions and agents, targeting, inter alia, the security forces. It is assumed that they have established connections with anarchist terrorist milieus in Italy - the Informal Anarchist Federation (Federazione Anarchica Informale, or FAI), and Greece – the Conspiracy of Cells of Fire (Synomosia Pyrinon tis Fotias, or CCF), whose modi operandi they partly imitate.

**Governmental PVE Strategies**

Due to the fact that major terrorist attacks, such as the 2015 Charlie Hebdo incident, and the following year the major incidents in Paris (Bataclan) and Nice took place, and due to the fact that many French foreign fighters departed for Iraq and Syria in order to join ISIS, the French government elaborated since 2014 several counterterrorism plans, including the Action Plan Against Terrorism (which was updated in July 2017). This plan was created by the National Coordination of Intelligence and of the Fight Against Terrorism (La Coordination Nationale du Renseignement et de la Lutte Contre le Terrorisme) and is directly supervised by the French president, providing counterterrorism coordination on the highest level.
On an institutional level, the Anti-Terror Coordination Unit (Unité de Coordination de la Lutte Antiterroriste, or UCLAT) is seeking to prevent terrorist threats. In contrast to some other democratic countries, France allows UCLAT to conduct surveillance of smartphones of suspected persons and to gain physical admission to their electronic devices. Citizens can report suspects to the National Center for Assistance and Prevention of Radicalization (Centre National d’Assistance et de Prévention de la Radicalisation, or CNAPR). This initiative led to thousands of calls on suspect activities and persons right from its start; currently data of some 20,000 persons have been collected in a database for the prevention of radicalization, the ‘File of alerts for the prevention of terrorist radicalization’ (Fichier des signalements pour la radicalisation à caractère terroriste or FSPRT). More than 11,000 persons have been monitored, with 4,000 of them being given the label “pre-terrorist.” This form of prevention of radicalization has been criticized because of the large number of “persons of interest” in relation to the actual threat level within the country.

Unlike some other Western countries, France’s approach to the prevention of radicalization also contains repressive components. The French parliament passed seven major laws on terrorism since the establishment of ISIS. These laws include, for instance, banning convicted jihadists from leaving France, expanded surveillance, the shutting down of jihadist homepages and heavy sentences for participation in terrorist groups, as well as for preparatory acts that might lead to terrorism, with sentences ranging from three to five years in prison for offenders. Since 2018, approximately 1,600 persons have been prosecuted or investigated with regard to jihadist activities. Attempts by French jihadists to join ISIS in Syria can lead to sentences of up to ten years and assistance in ISIS armed operations can lead to sentences of 30 years in prison. In 2018, a governmental plan to create an improved national counterterrorist office was initiated.

Efforts towards the prevention of radicalization in France have, in recent years, moved towards resilience-building directed at the internet, focusing on web content and users. The Inter-ministerial Committee for the Prevention of Crime and Radicalization (Comité Interministériel de la Prévention de la Déliquance et de la Radicalisation, or CIPDR) coordinates counterradicalization initiatives within France, providing training and supporting resilience-building measures. Until 2016, it invested over €90 million for the support of civil society efforts towards de-radicalization, but was accused of mismanagement by members of the French Senate in 2017. In 2018, CIPDR’s efforts shifted from de-radicalization to disengagement. Its new plan focuses on secondary prevention and on community-building, encompassing sports clubs in addition to schools and universities.

Selected French Literature on Radicalization and the Prevention of Radicalization

The book Preventing jihadist violence: The paradoxes of a security model (Prévenir la violence djihadiste. Les paradoxes d’un modèle sécuritaire) by Romain Sèze addresses French prevention policies since 2014; it is a very good example of critical research. Starting with the question of a proper definition of jihadist radicalization, Sèze discusses the development of various forms of governmental risk management in this area. A very interesting aspect is the author’s critical discussion of attempts of the French government to create a French Islam (Islam de France) or a republican Islam (Islam républicain) as an answer to Muslim radicalization. Sèze understands radicalization as a broad concept (concept 304radicaliz) that can become a self-fulfilling prophecy if not wisely handled.

Gilles Kepel and Olivier Roy are the most prominent French researchers on militant Islam, but their positions are very much opposed to each other. Kepel did field-research in the French suburbs (les banlieues) since the 1980s. He identified a combination of poor education, racism-linked deprivation, and economic hardship among Muslim immigrants, making it difficult for them to integrate into French society. Kepel examined the motives for the
radicalization of young adults within various (international) radical Islamic movements\textsuperscript{165} and Salafist groups.\textsuperscript{166} As a result of his field-research in French prisons and in the banlieues, Kepel found that both environments were recruiting-areas for ISIS in France.\textsuperscript{167} He describes the Islamist practices of many young French Muslims as a rejection of secular society (\textit{laïcité}) and noted their penchant for the use of violence, as illustrated by the many young French Muslims who departed for Syria, attracted by the Islamic State.\textsuperscript{168}

Like Gilles Kepel, Olivier Roy has observed radical Islamic movements since the 1980s. However, he concludes that young Muslims did not radicalize because of a lack of integration into French society. Rather, he found that radicalization is mainly a form of protest and provocation and part of a process to sever ties with their own parents.\textsuperscript{169} For Roy, this phase of youth development among many young Muslims in French diasporas has been responsible for the tendency of a number of them to turn to a fundamentalist version of Islam as a more congenial environment for their situation.\textsuperscript{170}

According to Roy, phantasies of violence and a suicide-inclination of militant young French Muslims, should be seen as the main drivers for them wanting to join jihadist groups, rather than an Islamist ideology.\textsuperscript{171} Roy rejects the thesis that the marginalization of young Muslims in the \textit{banlieues} and their discrimination are the main push factors for those who join the jihadist movement. He notes that the majority of the inhabitants of the \textit{banlieues} have remained peaceful.\textsuperscript{172} Roy also points to the fact that many of the jihadists have been criminal delinquents before becoming violent political extremists. Their inability to make something positive with their lives produces a kind of self-hate. As a liberation from their criminal past, a catharsis through embracing militant jihad offers many of them a way to gain, or re-gain, self-esteem.\textsuperscript{173} Due to its heterogeneity, Roy subsumes the current Salafistic movement under the term neo-fundamentalism. It includes a conservative wing that is based on a Wahhabi (Saudi Arabian) interpretation of Islam, and a jihadist wing based on militant Salafism.\textsuperscript{174} For Roy, the modern Salafiyya seeks to resurrect the former hegemony of Islam, whereas the Wahhabiyya is characterized more by its hostility toward the current (modern) world.

Roy sees the motivation for the violence of young Muslims from the banlieues as being based on their situation of individual hopelessness (e.g. regarding getting a decent job) and labels this process the “Islamization of radicalism” for the “negative heroes” who are challenged by society. Kepel, on the other hand, identifies a “radicalization of Islam” in the acts of many young French Muslims. Kepel sees their wish to participate in the establishment of a “caliphate” as a result of their fundamentalist understanding of Islam.\textsuperscript{175}

Next to Kepel and Roy, Farhad Khosrokhavar is another important field researcher. He explores Islamic radicalization in French prisons\textsuperscript{176} and also outlines several potentially fruitful approaches to prevention.\textsuperscript{177} As a sociologist, he explores changes in the interest of young Muslims for engaging in militant jihad in Europe and beyond.\textsuperscript{178}

McLaughlin’s work “Thinking about political 305adicalization in France” (\textit{Penser la radicalization politique en France}) provides an alternative approach regarding the roots of radicalization and jihadism (e.g. racial discrimination). He suggests a change of prevention policy in France in terms of a larger investment in education, and in enhancing psychological approaches.\textsuperscript{179}

Laurent Bonelli and Fabien Carrié’s work, \textit{The fabric of radicality: A sociology of young French jihadists} (\textit{La Fabrique de la radicalité. Une sociologie des jeunes djihadistes français}) examined 133 law suits brought against French jihadists in order to identify from the court documents he studied early signals of their initial radicalization and their growing interest in terrorism and in becoming foreign fighters.\textsuperscript{180}

The study \textit{The Revenants – They had gone to jihad, they are back in France} (\textit{Les Revenants. Ils étaient partis faire le jihad, ils sont de retour en France}) by David Thomson,\textsuperscript{181} an expert in the field of French and Tunisian jihadism, provides useful insights in the motivation of French FTFs/returnees and proposes new prevention approaches for this vulnerable group.
There are many governmental and non-governmental efforts to prevent radicalization in France. Three of these stand out:

1. **Artemis Association**: This governmental program tries to prevent pre-school children from falling under the influence of radicalized family members by strengthening their bonds with relatives who still feel a sense of loyalty to French society.  

2. **Plateforme d’harmonisation, de recoupement et d’orientation des signalements (Platform of harmonization, cross-checking, and orientation of reports – PHAROS)**: This governmental platform serves to locate and neutralize illegal online Internet content which seeks to glorify violence and engages in hate speech. Citizens are invited to report their observations on inappropriate Internet content to the authorities via PHAROS.

3. **Stop Djihadisme (Stop Jihadism)**: This governmental campaign was initiated after the attack on the satirical magazine Charlie Hebdo in 2015. It provides both online (via Facebook and Twitter) and offline contacts and prepares counternarrative programs for schools and prisons. In 2016, it launched a well-known project called “Toujours le choix” about two young adults on their way to radicalization that offers several exit options for those undergoing a radicalization process.

Many governmental PVE approaches in France adopt the penitentiary point of view of the Penitentiary Administration of the French Ministry of Justice and are lacking in more preventive approaches. Some of the law enforcement measures could be seen as problematic for young Muslims who want to provoke others in their environment, but are not attracted to violence themselves. Giving harsh punishments, such as a prison sentence, to young Muslims who speak positively about IS, may lead to "solidarization effects" and further radicalization.

French authorities had not considered the impact of religion in terms of extremism until the 1980s. It would appear that they are still not fully aware of appropriate PVE strategies in cases of religious extremism, due to its constitutional principle, that “religion is excluded from the republican way of thinking in France.” This stance - which was originally introduced to promote the equality of all French citizens - can be an obstacle when it comes to the prevention of radicalization. This is shown e.g. as in one case, when a moderate Rabbi and a moderate Imam were banned from talking to school classes, because they represent religions and wear religious clothing. If schools ban religious education, they surrender the interpretational sovereignty to outside religious leaders, who may, in some cases, be fundamentalists. With regard to religious radicalization, this could be prevented by introducing regular educational workshops on specific religions in French schools, led by teachers rather than clerics, in line with the concept of laïcité.

France appears to have a high number of female Muslims who travelled to Syria to join ISIS: 33 percent of the 1,324 individuals who travelled from France since 2012 were women. The share of young women and even minors involved in terrorist plots in France could point to the need for a larger investment in educational work by schools and communities.

Similar to the UK and Denmark, France’s returnee policy is inflexible, lacking a deeper understanding of initial radicalization motivations of vulnerable young men and women from diasporas, their subsequent rejection of the jihadist ideology, and their wish to be repatriated. With regard to a long-term PVE policy that is likely to reduce the interest in extremist ideologies, French authorities should therefore be considering changing the current hard-line policy towards the repatriation of FTFs and their children.
German Federal Republic

According to the German Federal Ministry of the Interior (Bundesministerium des Inneren, or BMI), 5.4 to 5.7 percent of the total population of Germany were Muslims in 2019. The projected percentage of Muslims of the total population in Germany in the year 2050 is estimated at 8.7 per cent (estimate with zero immigration), 10.8 per cent (estimate with medium immigration) 19.7 per cent (estimate with high immigration).

Germany was the primary destination country for asylum seekers from the Middle East, receiving 457,000 asylum requests from Iraqis and Syrians between mid-2010 and mid-2016. With hundreds of thousands of more persons seeking asylum in 2015-16, Germany became the top destination for refugees (86 per cent of whom were Muslim). Nevertheless, the share of people in Germany who hold that large numbers of refugees from countries such as Iraq and Syria are posing a “major threat” is among the lowest of all European countries surveyed (28 per cent).

In 2018, the German Higher Regional Court of Hamburg sentenced three Syrian nationals to long prison sentences for membership to a foreign terrorist organisation (ISIS) and (attempted) document forgery. Furthermore, the Court found that they were “part of an ISIS ‘sleeper cell’. (...) The Islamic State had arranged for them to travel to Germany with false passports, cash, and mobile phones in 2015, telling them to awaited orders for an attack.” In August of the same year, a 19-year-old Afghan national, who had applied for asylum in Germany, stabbed and severely wounded two American tourists in the Amsterdam central railway station, with a terrorist motive. He was arrested on the spot by police. In June 2018, a terrorist plot using ricin was discovered in Cologne, Germany. It was planned by a Tunisian citizen who was inspired by ISIS. He had tried to combine ricin with explosives, ball bearings, and bladed weapons.

An increasing number of offences against Turkish facilities such as shops and mosques, such as those which took place in Lauffen, Baden-Württemberg in 2018, by persons affiliated with the Kurdistan Workers’ Party (Partiya Karkeren Kurdistan - PKK) were interpreted as revenge acts for Turkish attacks on Kurds in Afrin, Syria. Against this background, collaboration between left-wing extremists and Kurdish organizations increased in various European countries.

According to the EU Terrorism Situation and Trend Report 2020, 59 arrests were related to terrorist offences in Germany in the year 2018; amongst them 43 for jihadist terrorism, eight for right-wing terrorism, five for ethno-nationalist and separatist terrorism (with ties to PKK), while the background of three remaining offences have not been specified. Two jihadist attacks occurred in the years 2017 to 2018, while another two jihadist terrorist plots were successfully disrupted. Eight attacks were completed but a number of suspects from right-wing terrorism in Germany could be foiled.

The German right-wing extremist movement is known for its attraction to weapons, explosives and the formation of neo-Nazi circles such as Comradeship (Kameradschaften). There exists also networks of sympathizers from the “intellectual right” as well as right-wing populist/extremist political parties, such as the Revolution Chemnitz group and the Empire Citizens Movement (Reichsbürgerbewegung). They mobilize discontent against migrants, such as in the case of an attack by members of the Revolution Chemnitz in September 2018. They target immigration policies as well political opponents, such as in the case of the Gruppe Freital (Freital Group) which attacked a left-wing politician. Members were found “guilty for leadership or membership within a terrorist organization, multiple attempted murders and grievous bodily harm.”

In June 2019, Walter Lübcke, a conservative politician who campaigned for refugees, was shot and killed by a right-wing actor in his own house. It is assumed that this “lone wolf” was not alone but part of a larger right-wing network. Ominously, in 2019, a right-wing extremist network was discovered within the German Federal Army’s (Bundeswehr’s) Special Forces Command (Kommando Spezialkräfte, or KSK), based in
Baden-Württemberg. Several members of the KSK hoarded weapons and explosives and planned an attack. Some of them were members of right-wing extremist groups such as Hannibal that seeks to attack Germany’s democratic system. In June 2020, the German Ministry of Defense dissolved the KSK unit. Furthermore, a rise of anti-Semitic attacks such as the one in Halle in 2019, has been attributed to the German right-wing milieu.

There is also a transnational left-wing and anarchist movement in Germany which includes environmental activists. They collaborate with members of violent anti-fascist movements in Denmark, Sweden, and Norway, as well as with left-wing and anarchist extremist persons and groups from Greece. Germany appears to have experienced the highest proportion (33 per cent) of returning foreign fighters (FTFs). Between 2016 and 2018, the estimated number of violence-prone Islamists grew from 24,400 to 26,560 persons (9 percent).

**Governmental PVE Strategies**

In July 2016, a 10-point declaration called “Strengthening of democracy and prevention” (Demokratie und Prävention stärken), was launched by the German Federal Ministry for Family Affairs, Senior Citizens, Women and Youth (Bundesministerium für Familie, Senioren, Frauen und Jugend, or BMFSFJ) in cooperation with various municipalities. It seeks to exchange information between social scientists and practitioners within Germany. In addition, in the same year, a governmental strategy with the title “Prevention of Extremism and the Promotion of Democracy” (Strategie der Bundesregierung zur Extremismusprävention und Demokratieförderung) was launched by the Ministry of the Interior (BMI) and the BMFSFJ. It involves the establishment of counselling structures on the local level and is meant to focus on vulnerable individuals. The federal prevention program Living Democracy! (Demokratie leben!) sponsors selected prevention ideas for persons at risk, their parents, and families as well as for youth work-related institutions and NGOs. 265 cities in Germany participate in this program, forming so-called Partnerships for Democracy (Partnerschaften für Demokratie, or PfD). In addition, various types of counselling, including for victims, are offered in cooperation with local democracy centres. Specific project ideas on the prevention of radicalization are sponsored by Living Democracy! In 2018, it sponsored 47 projects on the prevention of Islamic extremism.

A National Prevention Program against Islamic Extremism (Nationales Präventionsprogramm gegen islamistischen Extremismus, or NPP) was launched in 2017. It is administered by the BMFSFJ and BMI, with support from other governmental departments such as the Federal Ministry for Education and Research (Bundesministerium für Bildung und Forschung, or BMBF) and the representative for Migration, Refugees and Integration (IntB). The prevention concept of NPP combines elements of repression and prevention. It is a partnership between civil society organizations and government, with a budget of €100 million in 2018. It identifies focal points for prevention such as communities, mosques, and also focuses on prevention and deradicalization in prisons and in the probation service, and maintains a network of counselling and information points.

These federal PVE approaches must be seen in relation to the governmental claim for the continuous evaluation of their measures in order to improve quality standards in a fast-changing environment. The National Center for Crime Prevention (Nationales Zentrum für Kriminalitätsprävention, or NZK) was commissioned to assess this goal by the “Development of Evaluation Criteria for the Prevention of Extremism.” This assessment led to the publication...
Evaluation Criteria for the Prevention of Islam- Evls. This remarkable document identified 38 indicators to detect potential Islamist radicalization.212

In addition to government-driven approaches, various NGOs such as Ufuq or Violence Prevention Network (VPN) are working in the area of prevention of radicalization. These NGOs provide workshops, offer training sessions, distribute literature, and develop information programs (e.g. Inshallah Online - How religious extremists use the internet and what we can do against this, (Inshallah Online - Wie religiöse Extremisten das Internet nutzen und was wir dagegen tun können).213

Although there have been a number of evaluations of governmental prevention programs so far,214 there still exists a wider lack of evaluation initiatives within the field of NGO prevention organizations. In order to provide more “best practice cases” for new employees of these organizations and in order to assess which prevention methods work and which do not, it would be good to begin evaluations within these organizations.215

In Germany a distinction is often made between prevention of violence, and prevention of radicalization.216 The first deals with violent incidents, whereas the second tries to prevent the development of radical ideologies.217 Regarding the latter, it is important to enhance the skills of the employees of prevention initiatives, increasing their levels of expertise and to support them with best practice examples of radicalization cases. They also ought to be given better religious knowledge, e.g. by offering them assistance from Islamic theologians who graduated in Germany, in order to strengthen their position when arguing with young Muslims.218

Some of the major causes for radicalization within Germany are deprivation and prejudices (Islamophobia) since these may cause a loss of a sense of belonging and an intensive search for identity among vulnerable young adults.219 For this reason, a psychosocial approach towards the prevention of radicalization is seen as a key element by several German researchers in this field.220 There are many governmental and non-governmental efforts to prevent radicalization in Germany. Three of these stand out:

1. **Datteltäter:** This civil society initiative was established in 2015 as a humorous response to the rise of ISIS. Its founders are five young Germans who themselves also have ties to Islam or share a migration background. Datteltäter [Date perpetrator] focuses on prejudices towards Muslims and Islam but also tries to confront and prevent Islamic fundamentalism with the help of satire. Due to its use of various social media platforms and its authentic approach, it has gained several media awards and is very popular among young German adults.221

2. **German Institute of Radicalization and De-radicalization Studies (GIRDS):** GIRDS focuses on theoretical research as well as practical work. It offers training on de-radicalization and supports other organizations in the development of counterradicalization initiatives and advises these organizations on issues such as re-radicalization while also providing expertise for the evaluation of ongoing projects.222

3. **NEXUS:** Nexus is part of a project on Prävention und Deradikalisierung in Strafvollzug und Bewährungshilfe (Prevention and De-radicalization in Prisons and Probation Services), and is operated by BMFSFJ, VPN, the NGO Denkzeit-Gesellschaft (Thinking Time Society), and the research group Modellprojekte e.V. (Model Projects e.V.). It offers psychological support for prisoners and their families with the help of the union for the prevention of extremism in Berlin.223

Islamist extremism and its prevention are targeted by 32 percent of the P/CVE programs in Germany.224 Half of all these programs mostly target children and adolescents in critical periods of their lives, in order to help them form an identity and provide them with a sense of belonging, as well as in order to strengthen their resilience against radicalization.225 Experiences of discrimination such as Islamophobia are high risk factors for radicalization in
Germany. Due to the fact that the majority of radical Islamic movements belong to a non-violent puritan social environment, the major aims of 75 per cent of PVE programs in Germany focus on knowledge transfer and educational work and deal with youth, (social) professions and civil society in the context of primary prevention. Only few PVE program providers such as VPN, offer additional secondary and tertiary prevention programs (including de-radicalization and opt-out-programs) such as the Coordination and Advisory Center for the Prevention of Radicalisation (KORA).226

One of the challenges for many German PVE programs is the lack of external or internal evaluations, as Gansewig and Walsh found in their study about the utilization of “formers” from extremist milieus in PVE projects.227 It was found that 15 per cent of the German projects did not carry out an evaluation in 2017.228 Therefore, the NZK recommends the integration of quality guidelines such as the Beccaria Standard,229 already in a project’s planning stage.230

It is notable that family counselling is hardly a focus in German PVE projects though there is a manifest need for such counselling.231 Germany counts a large number of Muslim communities with ties to Turkey and other Muslim countries such as Morocco. Some of the young adults from these communities do not only participate in an Islamist movement but also in ethno-nationalist and separatist movements. Yet others are linked to organized crime. It is important to increase support for the families affected by this and to involve them in PVE strategies to counter extremism.

The United Kingdom

In the UK, 6.3 per cent of the total population were Muslims in the year 2016.232 The projected percentage of Muslims of the total population in the UK in the year 2050 is estimated at 9.7 per cent (estimate with zero immigration), 16.7 per cent (estimate with medium immigration) 17.2 per cent (estimate with high immigration).233 43 per cent of recent migrants into the UK were Muslims.234 According to a survey of the Pew Research Data, 80 per cent of British people who have a negative opinion of Muslims said that the high number of refugees from Iraq and Syria represent a major threat.235 However, only 17,000 asylum seekers from Iraq and Syria were counted in the UK whereas 457,000 asylum seekers reached Germany at the same time.236

According to Europol’s EU Terrorism Situation and Trend Report, 281 terrorism-related arrests between 2015 and 2019 have been reported in the UK (not including Northern Ireland).237 With regard to right-wing terrorist attacks, one completed attack and three foiled plots were recorded in the UK in 2019 (not including ethno-nationalist attacks in Northern Ireland).238

Governmental PVE Strategies

Since the 7/7 bombing of 2005 which targeted people in London transport, the British government has developed four “pillars” that form the UK’s government CVE policy CONTEST:

1. Prevent the ideological challenge of terrorism;239
2. Pursue (stopping terrorist attacks happening in the UK and overseas)
3. Protect against a terrorist attack in the UK or overseas;
4. Prepare to mitigate the impact of a terrorist incident if it occurs.240

Prevent costs nearly £40m per year and is meant to prevent young people from joining terrorism-related activities or supporting these activities, focusing on the “pre-criminal space.”241 It includes training for public sector workers and frontline practitioners such as
nurses, probation officers, doctors, teachers, and university lecturers in order to prevent radicalization. Through the “Counter-Terrorism and Security Act 2015,” Prevent became a legal obligation, the frequency of trainings increased, including in the private sector, as in the case of cooperation with the fast food chain McDonald’s. Prevent will be discussed in more detail below. When it was initiated, its approach was unique among Europe’s PVE strategies; it was also exported to other countries.

Prevent is accompanied by a program termed Channel. It means a Prevent referral will be indicated, for instance based on a recommendation of a general practitioner whose patient might have shown “signs of radicalisation.” Such a “case will be screened by the Prevent lead within the organisation, often a safeguarding professional.” The police will examine whether the person who might be at risk of radicalization is not already part of “an active counter-terrorism investigation” and will check the motivation based on the “3M test” (“misguided, malicious or misinformed”).

After that process, the case might be discussed in a Channel panel meeting, a multi-agency assembly that is led by the police; it involves various representatives, e.g., from health, education, or local authorities in the decision-making procedure. At this stage, a check regarding specific needs of a “pre-radicalized” person (such as mental health support) would not yet have taken place.

With regard to Prevent and the Channel process, Aked criticizes the fact that only between five and ten per cent of the total amount of all Prevent referrals led to the Channel panel, whereas between 90 and 95 per cent of the referrals have been marked as “false positives” by the police. Regardless of the fact that some “Prevent cases never reached a Channel panel, all of the referrals are recorded in a Prevent Case Management (PCM) database, and reportedly stored for seven years.”

Although over 1,500 individuals have been brought into the Channel program since 2012, the exact content of the program is still kept secret. The BBC compared it with a system of “re-education,” while the Home Office calls it “ideological mentoring,” claiming also that participation is “voluntary and confidential.”

The report “False Positives: The Prevent counter-extremism policy in healthcare” addressed some of the problems found, including a suspected correlation between mental health issues of certain individuals and their engagement in violent extremism or terrorism. The report found that:

“The evidence for official claims that people with mental health conditions are more likely to be drawn into terrorism is not robust enough to base policy upon. […] some mental health specialists believe the claim risks pathologisation and exacerbating stigma.”

In addition, the report criticized the pressure on health workers by authorities “to navigate [and] to comply, and to refer, often without consent.” It was reported that many were “deeply concerned about the possibility of a broader erosion of trust and some are concerned about criminalization in the context of all Prevent referral data being recorded on a police database.” The report concluded that the Prevent policy in healthcare rests on “grey areas, a lack of clarity, conflation of safeguarding with public protection and a failure to distinguish between “vulnerable” patients and patients lacking capacity.” The large variation in Prevent referrals and the false positives rates across the National Health Service (NHS) “was considered as problematic.” Another result of the study was that Prevent might contribute to discrimination of two groups in the UK: Asian communities and Muslims. Asians were referred four times more often than non-Asians. Muslims were referred eight times more than non-Muslims. In addition, Aked’s report on Prevent found that “it stigmatizes people with mental health conditions, and often damages the care they receive. There is also strong
evidence that Prevent is damaging presumption of patient consent and confidential medical
care, and trust in the medical profession.\textsuperscript{261}

The Prevent training materials include indicators of possible signs of radicalization that are
built on elements of the “Extremism Risk Guidance 22+” (ERG22+), also known as Channel
Vulnerability Assessment Framework.\textsuperscript{262} They were based on just one psychological study that
identified 22 factors (“Engagement factors,” “Intent factors,” and “Capability factors”) considered as possible radicalization indicators.\textsuperscript{263} Although this framework has been
embedded in Prevent since 2011, it was classified until 2015 and the underlying assumptions
were never made public, which makes the reliability and validity of it difficult to assess.\textsuperscript{264}

According to the UN’s Special Rapporteur on the promotion and protection of human
rights and fundamental freedoms while countering terrorism:

“Psychometric systems like the ERG22+ “mix structured forensic analysis
models, traditionally focused on mental illness and deviance, with other
models of intelligence analysis containing strong ideological and political
connotations” and “consistently use ambiguous factors in their
application.”\textsuperscript{265}

While the Home Office claimed that 85 per cent of the Channel participants had emerged
from the programme without any future interest in radicalization,\textsuperscript{266} its efficacy is empirically
unverifiable from the outside. Several former participants, e.g. the Parsons Green bomber\textsuperscript{267}
who had been flagged to Prevent, or the perpetrator of the London
Bridge attack in December
2019, who had completed this program, were clearly not de-radicalized.\textsuperscript{268}

\textbf{Selected Review of the British Literature on Radicalization and the Prevention of
Radicalization}

An outstanding study on the development of ISIS-related radicalization in Britain as well as
on prevention possibilities, is titled \textit{The Islamic State in Britain. Radicalization and Resilience
in an Activist Network} and authored by Michael Kenney in 2018. He suggested that:

“Britain and other Western democracies can continue to deal with the threat of
violent extremism without sacrificing the political rights and civil liberties that
sustain their own identities as democratic societies. Part of the solution is to
allow groups that engage in peaceful protest the room to express their
grievances lawfully. This is part and parcel of what makes Britain great.”\textsuperscript{269}

Kenney’s approach aims to actively include British Muslims as citizens of the UK in the
process of preventing and countering radicalization – an approach also advocated in other
studies\textsuperscript{270} which do not stereotype members of Muslim diasporas as “enemies” of British
values.\textsuperscript{271} According to Heath-Kelly, the “othering” of British Muslims has been a result of
various jihadist attacks in Britain. But this “othering” can lead to a solidarization of young
Muslims and converts with radical Islamist groups.\textsuperscript{272} More recent initiatives by the British
government indicate a shift from a repressive to a preventive approach, and often include a
focus on family counselling to prevent radicalization.\textsuperscript{273}

The study titled “I left to be closer to Allah. Learning about Foreign Fighters from Family
and Friends” by Amarasingam and Dawson, also emphasizes the need for the involvement of
family and friends in prevention and deradicalization approaches.\textsuperscript{274} Sadek Hamid’s work “The
Attraction of ‘Authentic’ Islam. Salafism and British Muslim Youth”\textsuperscript{275} discusses the search
of young British Muslims for a non-traditional, but “pure” Islam. He underlines the importance
of a “shelter” which a (strict) religious community can offer to young adults in the face of daily
discrimination while they are torn between familial traditions, societal expectations, political pressure, and individual wishes.

Sarah Marsden, in her book *Terrorist Recidivism: Deradicalisation and Reintegration*, underlines the need “to focus on addressing perceived misinterpretations of religion, or attempting to modify emotional responses to perceived injustice to encourage people to pursue those same goods in pro-social ways.” She recommends a “Good Lives Model” - a concept that contains both values and personal agency, in order to combat terrorism - and to pay closer attention to individuals in their social and political context in order to secure better outcomes.

In part of the British literature on the subject there is a major focus on prevention within educational settings, based on “the idea that access to quality education for all students, regardless of gender, culture, faith, nationality or ethnicity, is the starting point for PVE.” A fine account on this topic can be found in Taylor and Soni’s “Preventing Radicalisation: a Systematic Review of Literature considering the Lived Experiences of the UK’s Prevent Strategy in Educational Settings.” Afia Ahmed Chaudhry’s dissertation “Resisting Radicalisation: The Impact of the Prevent Duty on Teacher-Student Relationships” is field-research based and raises pertinent questions with regard to the usefulness of prevention initiatives in schools or by teachers. Chaudhry observes: “it is perhaps important to note the way teachers engage with this topic because it encourages the need for critical and honest debate, spearheaded by those directly impacted by government policy.”

With regard to the prevention of radicalization within schools and universities, there are a number of notable studies. There has been a growth of Islamic NGOs which claim to be able to prevent and de-radicalize their fellow believers, which, in turn, has led to criticism from others in Muslim communities. Many Muslims do not see the benefits of a pedagogical approach, with some of them viewing this as a new form of governmental surveillance of Muslims in so-called “safe spaces,” with racist implications. Indeed, there have been a few cases identified where teachers or social workers have been unmasked as counterterrorism officers. This has led to a higher level of mistrust towards such education-based initiatives, and, possibly, also contributed to radicalization.

There are many governmental and non-governmental initiatives to prevent radicalization in the UK. Three of these stand out:

1. **The Active Change Foundation (ACF):** This initiative was led by its founder Hanif Qadir, a former radical-Islamic activist, and his team from 2005 until 2019. It aimed to empower young Muslims and to prevent them from being attracted by radical Islamist ideas. One well-known initiative of the ACF was its campaign #NotinmyName. Like some other groups, the ACF has been accused by some members from Muslim communities of conducting surveillance for the intelligence service and many participants became mistrustful and left the foundation.

2. **Project Generation Global (the Tony Blair Institute for Global Change):** This project offers training for teachers to facilitate dialogue in the classroom in order to create “safe spaces.” It tries to connect classrooms across the globe and helps students to navigate their problems in a positive way.

3. **Imams Online:** This initiative tries to prevent radicalization through imparting Islamic knowledge by recognized religious authorities.

Ahmed Patel, the brother-in-law of the former London 7/7 bomber Mohammed Siddique, is an excellent example of a British Muslim who stood up against religious radicalization. From an outside observer’s perspective, it would appear that people like Patel are authentic actors in the field of prevention work and should therefore be included to a greater extent in British (non-) governmental PVE approaches.

According to Lloyd and Dean, guidelines for assessing risk in extremist offenders are necessary in order to prevent recidivism. Although it would appear that the Home Office has
changed its strategy toward some elements of the original program\textsuperscript{295} in the case of Prevent, many elements are still unknown and may remain so for some time. This lack of transparency, in combination with the terrorist attacks by former participants in this program, does not increase trust in its efficacy.

Lessons Learned

In the following, a selection of outstanding national PVE approaches will be discussed. These could be applied, or at least helpful, for the improvement of such approaches in other countries. A good example for a promising PVE approach is DERAD, a project of eight institutions from six European countries aimed at the prevention of radicalization in prisons.\textsuperscript{296} It supports imprisoned political offenders as well as officers guarding them, warning the latter about the risks of jihadist recruitment in general and individual radicalization processes in particular. As a large-scale program with a broad online menu, it supports prison and probation officers as well as officials from judiciaries, translation services, law enforcement agencies, and other stakeholders. Furthermore, DERAD provides recommendations based on court decisions across Europe and offers advice regarding social rehabilitation. One spin-off of DERAD is HERMES,\textsuperscript{297} a platform for interactive training for CVE-activities.

Two other good examples in the field of CVE and PVE deserve to be mentioned. The first is the European Commission’s Radicalisation Awareness Network (RAN)\textsuperscript{298} which was established in 2011 and currently includes several thousand stakeholders from academia, government, and civil society, including many social workers. RAN offers a broad range of workshops and activities for the exchange of good practices among participants.

One of the main participant groups of RAN are consultants involved in preventing and countering radicalization that leads to violent extremism, especially on the municipal level within Europe. RAN organizes working groups related to specific topics or professions such as prison and probation workers. Such groups meet on- and offline and exchange information about challenges and new approaches. Their experiences and recommendations are gathered in reports and so-called “Collection of practices” - a selection of best practices which are freely available on the internet.

One of the best studies about female radicalization with regard to ISIS in Europe and abroad, is the book *Guest House for Young Widows - Among the Women of ISIS* by Azadeh Moaveni.\textsuperscript{299} It highlights the fate of several girls from their initial radicalization in their countries of origins, to their departure for joining ISIS in Syria and Iraq and their escape from the terrorist organization. In addition, it sketches a critical picture of their social and political circumstances as well as their interest in religion. The different reasons for girls and young women from the “West” and the “East” for radicalization are identified, without losing sight of the individuality of decision-making by these female jihadists. One key finding of the book with regard to the prevention of radicalization is the fact that Muslims, who are socially and religiously conservative, should not automatically be viewed by governments as extremists and treated as such. Otherwise, the alienation of Muslimas which is often based on the absence of a self-determined life perspective, might make them even more vulnerable to radicalization.\textsuperscript{300}

Conclusion

This overview of various efforts towards the prevention of radicalization in Western Muslim diasporas in five countries has shown that over the years there has been a shift from CVE to PVE. The initial, more repressive, CVE approach was the result of a series of terrorist attacks in Europe and North America and was meant to restore a sense of security among citizens. Strict law enforcement and the frequent stereotyping of members of one religion as potential
“enemies” did not bring about a decline in radicalization or a greater identification of diaspora members with the cultural and political values of Western societies. Rather, it led to a new wave of clashes with the host country’s traditional values, and to new forms of radicalization and further attacks, partly driven by growing Islamophobia, and partly driven by a continuing search for belonging which the former “Islamic State” initially seemed to satisfy. The old truism that “violence begets violence” became true again, e.g., in France, where various special armed police units such as the Sentinelle, while meant to restore public security, were also seen as provocation by some members of Muslim communities. Furthermore, their presence did apparently not significantly reduce the number of attacks in France, or lead to a decline in numbers of radicalized French citizens and residents. Terrorist attacks in Britain could not all be prevented by the extensive public surveillance put in place, but seemed to “provoke” or - even worse - to “attract” some social media “addicted” jihadists who wish to see themselves being video-taped during their attacks in order to become “famous” in the online Jihadi scene.

The idea of monitoring one section of the public and inviting citizens to report on their neighbours’ activities leaves a bitter taste, especially in those countries which experienced Fascist rule in the not so distant past. While the idea to prevent terrorist attacks with the help of civil society involvement and citizens’ awareness of radicalization symptoms in their neighbourhood is based on good intentions and can be made to work, as exemplified by the Danish Aarhus model, it is a double-edged sword as it can also lead to greater mistrust between host society and diasporas, fan religion-based prejudices, and provoke vigilantism in the form of right-wing racist actions.

In recent years, it has become quite clear that a long-term solution for the problem of radicalization has to be sought in preventive approaches at various levels. An example of this could be the initiative of the European Commission termed EU Cities against Radicalisation. Radicalization does not come out of the blue but is, in the majority of cases, the result of persistent discrimination, deprivation, and the absence of societal and political participation. Vulnerable persons have to be approached by others who do not judge them beforehand, but are willing to listen and help them to discover the various pull and push factors behind their attraction to extremist ideas. Professional assistance, based on psychosocial approaches, appears to be the way forward to show vulnerable people how to make something of their own lives without feeling the need to destroy the lives of others to feel empowered themselves.

Successful PVE approaches are usually based on the cooperation of experts from academia with practitioners such as street workers. In addition to skilled social workers and trained psychologists, such combined efforts can also include individual police officers who are well-known and trusted within the community.

The CVE approach became for a while “big business” in some of the countries discussed. However, many initiatives were often mismanaged and less than sensitive to the actual needs of the targeted groups. According to Johansen, many CVE “experts” have been randomly selected for the task. In some cases, they were chosen because of their skills to manage risk in different domains, such as youth crime prevention, protection of children’s well-being, or the prevention of substance abuse among homeless and mentally disadvantaged groups.

This review of the P/CVE-approaches in the five Western countries highlights that in reality several of the initiatives in the field of CVE were not able to provide adequate help. It is important not to repeat the same mistakes in the growing field of PVE.

The key element of PVE should be the willingness to understand the real needs of vulnerable individuals and groups in diasporas so that adequate assistance can be provided. PVE approaches should be able to challenge fundamentalist religious narratives in various spheres of life - such as schools, families, sport clubs, mosques, and on the internet - and try to offer constructive and persuasive alternative religious and non-religious narratives. This can only be achieved when and where credible narratives are provided by authentic “role
models” whether these are (quietist) religious authorities, peer-group members with street credibility, or highly-regarded individuals from local communities. The best PVE initiatives respond to actual needs by combining religious, social, psychological, academic, and criminological expertise. Such approaches ought to be based on a “living-together” approach that includes the “Good Lives Model” for everyone in society.

With regard to the various (non-)governmental approaches of prevention within the five countries that have been briefly discussed in this chapter, it might be wise to abandon the idea that it is possible to invent a national Islam (be it French or German) or a Euro-Islam. It should be accepted by Western democracies that religious affiliation and practice, freedom of thought, and belief is a private matter and a human right. The inalienable rights of religious freedom and freedom of speech should be granted to everyone, regardless of their religious affiliation. Conservative religiosity is not synonymous with fundamentalism nor is it linked to terrorism. Not every statement of young Muslims about ISIS should necessarily be seen as “real” sympathy for violence, but might just be an expression of youth “rebellion” against their social environment.

In this context, we should also ask ourselves whether the term “Western Muslim Diasporas” is not already a form of “othering,” implying that Muslims could never be “real” citizens of Western countries because their “real” loyalties lie elsewhere. The othering of Muslims who in their majority have become Western citizens makes them more vulnerable to radical recruiters. This vicious circle can only be interrupted by strengthening the national ties of citizens with Islamic roots towards their Western homelands and through the support of their feeling of belonging to a specific Western society. According to Yasmeen, “the underlying rationale for the strategy is not to implicate all Muslims as terrorists,” because this assumption “unintentionally perpetuates the myth of an antagonistic relationship between Islam and the West. The very act of identifying Muslims as the “other” that needs to be engaged creates the space for those who are predisposed to viewing Islam and Muslims in negative terms.”

Another term is also problematic: “Islamist.” It is widely used in the fields of P/CVE. On the face of it, “Islamist” seems to be a suitable description for radical, fundamentalist, extremist, and terrorist approaches associated with the religion Islam, because the term seems to cover all of this. However, the use of this term might actually support recruiters for radical Islamic movements because it associates an entire world religion with terrorist attacks and implicitly criminalizes all believers - although most of them would never dream of getting involved in violent extremism or perpetrate terrorist attacks themselves. Lawyer and Islamic theologian Hamideh Mohagheghi sees an implicit combination of crime and religion in the term “Islamist,” one that is negatively influencing public perception of a particular religion. One wonders why such a link between a crime and a religious affiliation is not applied to acts of terrorism perpetrated by members of other religions, such as Christianity. In the US, a number of perpetrators of terrorist acts have been Christian fundamentalists, but nobody calls this phenomenon “Christianism” or their attacks “Christianistic.”

Within Europe, there is no common legal understanding of radicalization and extremism. This has led to diverse penalties for those considered radicalized and extremists. This has social and political consequences, such as when it comes to the “resocialization” of “formers” into their societies. For this as well as for other reasons, and in accordance with the EU’s External Action on Preventing and Countering Terrorism and Violent Extremism directive from June 2020, the cooperation between different (EU) countries regarding the internal and external dimensions of counterterrorism and prevention should be strengthened in order to build more effective synergies between these countries. It might be wise to consider the implementation of “uniform” PVE strategies and laws on (at least) a European level. By following a common strategy, without “regional or local exceptions”, the (sometimes) misleading approaches and effects that result from dissimilar P/CVE approaches could be avoided and the positive effects
of PVE measures in each country could be increased. This would be in line with a recent recommendation of the Council of the European Union regarding the use of strategic communication “to enhance EU efforts to prevent terrorism and violent extremism” and to “contribute to national and regional efforts to address terrorism and curtail the radicalisation and recruitment that bolster extremist groups.”

Seven Recommendations

Based on the research of the PVE strategies within the selected five European countries of this chapter and the author's own experiences in the field of prevention of jihadist radicalization, the following recommendations are offered with regard to the improvement of the effectiveness of future prevention of radicalization efforts and existing PVE approaches:

1. Resilience Assessment Tools

With regard to the debate of the possible repatriation of former foreign fighters and other returnees such as children, it might be wise to develop a Resilience Assessment Tool for first- and second-line practitioners e.g. probation officers, social and youth workers, teacher, as well as university lecturers who have to deal with vulnerable individuals in order to prevent recidivism to the jihadist milieu.

In addition, Resilience Assessment Tools have to be developed in a multi-disciplinary collaboration of religious scientists, law enforcement agencies, criminologists, and ethnologists with regard to the specific needs of the vulnerable returning groups. According to Orla Lynch, “trauma training should be a key component for interventionists/practitioners. This should involve a self-care component as well as awareness of trauma in clients.”

Currently, insufficient psychological support is provided to former foreign fighters and returnees in Europe. In addition, there is a shortage of polyglot therapists who are aware of the specific radicalization content and the experiences of members of jihadist groups. Therefore, it might be helpful for the reintegration of these individuals into their society to provide therapists who are able to talk to their clients in their mother tongues in order to provide a secure climate of communication.

Furthermore, it must be guaranteed that only female therapists will talk to female individuals who experienced violence by men, or refuse to talk to male therapists for religious reasons. The provision of specific therapies for traumatized children whose parents have a background of religious extremism is also essential.

Resilience Assessment Tools could be used, for example, for the evaluation of reintegration programs of former foreign fighters, as well as other returnees and their children, in order to assess their effectiveness and sustainability and to recommend, if necessary, modifications.

2. Create Support Groups for Formers and Returnees

Apart from psychological, pedagogical, and law enforcement approaches regarding formers and returnees, the development of support groups – led by repatriated and re-socialized formers or returnees - can be seen as an authentic approach to get in touch with these vulnerable persons and make sure that they feel understood. In contrast to professional support situations with clearly defined roles such as “therapists” and “clients”, a low threshold connection between individuals who experienced similar radicalization processes or experienced fascination for violence themselves, could enable formers and returnees to open up, exchange information with each other on their daily frustrations and experiences, and talk about their fear of
recidivism due to continuing links with their previous networks. Such support groups for formers and returnees are important and well-suited for the prevention of re-radicalization.

3. Support Groups for Parents and Siblings of Radicalized Individuals

There is also a need for the establishment of support groups for parents and siblings of (former) radicals in order to empower these, both for themselves as well as for their brothers, sisters and children. In contrast to family counselling that is often led by professionals or experts in these fields, this approach may be more likely to be successful if it could provide a “private sphere” or “protected places” for parents and siblings of radicalized individuals. There they could find some respite away from media attention, to exchange information, if they want to, and find others who experienced the same as they did. From this author’s perspective, this concept is comparable to the Alcoholics Anonymous (AA) groups where churches or public buildings provide places for AA to meet and where they can find a mentor who has “recovered.”

4. Invest in Family Counselling

According to Koehler, “Family matters far more in de-radicalization and counter-terrorism work than typically realized. (…) The social environment and within it, more specifically, close friends and family, is arguably one of the spaces in which violent radicalization takes place and becomes visible in early stages.” According to one study on lone actor terrorists, family as well as friends recognized the future perpetrator’s increasing interest in terrorism “in 63.9% of the cases because the offender verbally told them.” With regard to future PVE approaches in the field of jihadist radicalization, family counselling programs could be very useful for “pre-radicals,” because the family as a social unit and the internal family dynamics and individual driving forces behind violent radicalization can be targeted. In compliance with Koehler’s recommendations, various quality standards should be introduced for family counselling programs in the PVE environment. Furthermore, families should be treated “as partners in early prevention and even intervention work” and “not be seen as a source of intelligence and information for the authorities.”

5. Research on the Physical and Mental Health Impacts of Prevention Programs on their Clients

As has been pointed out by Aked, this area is seen as “chronically under-studied” and needs “further evidence,” especially with regard “to people with mental health conditions, […] BAME [Blacks, Asians and Minority Ethnics] groups, and children and young people.” It might be useful to adopt a strategy of “proportionate universalism” instead of focusing on specific individuals and to avoid the pathologization as well as discrimination against certain groups. In addition, funding for research on prevention programs appears to be a good step towards a more effective strategy based on justice and equality.

6. Greater Awareness of the Terminology in PVE Programs

With regard to PVE programs and projects, appropriate terminology is crucial. Currently, it seems to be quite “trendy” to integrate the term “religious related extremism” in the title of PVE approaches. Several projects have been funded that include this terminology. Critics from the Muslim community point out that “religious related extremism” is just a cloak for Islamic extremism. In fact, a large number of these projects cannot hide the fact that their main interest
lies in countering Islamic radicalization and they are solely interacting with Muslim communities but not with any other religious community. One example of this practice is the German federal government’s working committee Religious Related Extremism (Bundesarbeitsgemeinschaft religiöser begründeter Extremismus, or BAG RelEx), that was established in 2016 as an association with 26 civil society partners. In 2018, it still concentrated on “Islamic-related extremism.” This exclusive focus raises suspicions within Muslim communities. Some also fear potential cooperation of these PVE approaches with security services, e.g., in terms of providing personal data from members of Muslim communities or groups.

7. The Integration of Quietist Salafi Preachers in PVE Approaches

In Germany, another gap in the field of prevention of radicalization is the refusal of governmental PVE approaches to integrate quietist preachers from the Salafi milieu in prevention projects. In the view of this author, this is short-sighted. This author found that a number of quietist/puritan Salafist preachers whom she had interviewed did very good prevention work in their local environment, managing to dissuade a number of ISIS-sympathizers who wanted to become foreign fighters in Syria, thanks to their religious reasoning skills. They were certainly more successful and more interested in the needs of young Muslim adults than many imams from other Muslim associations such as, for instance, The Turkish-Islamic Union for Religious Affairs (Diyanet İşleri Türk İslam Birliği, or DITIB), the largest Islamic Union in Germany, controlled by the powerful Turkish government agency for religious affairs Diyanet, which “services” more than 900 communities and affiliates in Germany. Based on the author’s own experiences with many quietist preachers, they would recommend their integration into PVE approaches, because they are often more aware of the specific needs of the target groups who are at risk for being attracted to jihadism than anyone else, but deny violence as “un-Islamic” themselves.

The decision to include puritan Salafist preachers within prevention or de-radicalization work should certainly be decided on a case-by-case basis. With regard to this decision, Western societies should keep in mind that these preachers have great knowledge of Islam that could be very helpful when it comes to theological “debates” with radicalized individuals. The puritan Salafist preachers would not require a specific religious education, because they are already familiar with Islamic theology and sources – although their interpretation can certainly not be considered as “liberal.” But for the sake of avoiding Muslim teenagers and (young) adults killing and getting killed in the name of Islam, most of the puritan Salafist preachers can be seen as strong potential partners, because they also see jihadist movements such as ISIS as evil and describe them as anti-Islamic, due to ISIS’ focus on violence and “wrong” Islamic sources.

In the view of this author, puritan Salafist preachers could become strong allies of Western societies and help them in separating vulnerable Muslim youth from jihadist Salafist preachers. That is important, because puritan Salafist preachers are often themselves threatened physically by jihadist Salafist preachers and their followers, because – in contrast to the jihadist Salafist preachers - they stand up against violence in the name of Islam. Though this peaceful attitude of the puritan Salafist preachers is often not visible to the public, it could become more visible by their official acceptance by the government. This would support the daily prevention work of these Salafist preachers. Based on this author’s field-research in nine European countries, some experts are aware of the fact that various puritan Salafist preachers try to achieve respect for their prevention work within so called “secular” mosques whose imams they often support in terms of “de-radicalization.” However, so far, they often do not receive any personal or monetary credits for their Islamic “de-radicalization” and prevention work. This lack of recognition frustrates them a great deal. If governmental P/CVE approaches would officially include puritan Salafist preachers in their P/CVE programmes, this would, on the one hand,
strengthen their bond to Western societies and values. On the other hand, the experience of governmental respect and the recognition of being part of a “good cause” would surely be transferred into the P/CVE work of puritan Salafist preachers. Thereby the vicious circle of Muslim- or Islam-related discrimination - as one of the major drivers for radicalization in Western societies - could be broken. In sum, the integration of purist Salafist preachers into governmental P/CVE efforts should be seen as valuable for both diaspora youth at risk and Western societies as a whole.

Dr. Nina Käsehage is a Senior Lecturer at the Department of Religious Studies and Intercultural Theology, University of Rostock, Germany. Currently Nina Käsehage is preparing a ‘Habilitation’ on the religious socialization of children who were raised by the Islamic State. In 2017, she completed her doctoral dissertation ‘The current Salafi Scene in Germany - Preachers and Adherents’ (‘Die gegenwärtige salafistische Szene in Deutschland - Prediger und Anhänger’) at the Department of Religious Studies of Georg-August-University, Göttingen. Her thesis was based on more than one hundred in-depth interviews with Salafi preachers and members of groups such as Milatu Ibrahim (MI). More recently, she conducted 60 interviews with female Jihadists in nine European countries for her forthcoming book ‘Women in Jihad’ (‘Frauen im Dschihad’). She is a member of the German Association of Religious Studies (DVRW), the Commission for Diversity and Equality of the University of Rostock and the European Experts Network on Terrorism Issues (EENeT). She is also a member of the think-tank Cologne Forum for Domestic and Security Policy (KFBIS). In addition, she is the founding member of the scientific advisory board RadiPräv, a Göttingen-based organization for the prevention of religiously motivated radicalization. She also offers consulting services in the field of Salafism, Jihadism, Takfirism as well as religious radicalization.
Endnotes

1 A longer version of this chapter, including more case studies, has been published as: Käsehage, Nina (2020). *Prevention of Violent Extremism in Western Muslim Diasporas*, *Religionswissenschaft: Forschung und Wissenschaft*. Berlin and Zürich: LIT Verlag.


3 In this chapter, “prevention” and “Radicalization” relate solely to religion. It is important to underline this focus, because members of Muslim diasporas can also be radicalized by a secular ideology.


11 Ibid.


16 The real or imagined discrimination against Muslims in the “non-Islamic world” and abroad is also a strong motivation for converts to Islam to solidarize with the needs of “the” Islam. In cases of radicalization, it can be seen as a push-factor for the recruitment of new activists for violent ideologies. Cf. Kunst, Jonas R., and David L. Sam, ‘Relationship


18 European Commission Against Racism and Intolerance (ECRI) and Council of Europe ‘Annual Report on ECRI’s Activities Covering the Period from 1 January to 31 December 2018,’ *ECRI and Council of Europe*, 29, 2019, pp. 10ff. Conversely, “Westernphobia” may be discerned in religion related education within radical Islamic milieus among Europe. In contrast to “Islamophobia,” a phenomenon that is measurable in all societal milieus within ‘Western’ societies, “Westernphobia” is solely assessable within a minor field: the radical, religion-related environment.


20 Bayrakli and Hafez 2019, Foreword.

21 Ibid.

22 Ibid.


24 Ibid.


26 Jikeli 2018, p. 103.

27 Bayrakli and Hafez 2019, p. 12.


33 Cf. Pew Research Center, ‘Europe’s Growing Muslim Population. Muslims are projected to increase as a share of Europe’s migration – even with no future migration,’ Pew Research Centre, 29 November 2017, p. 5.

34 Tahir, Kunst, and Sam 2018, p. 2.


36 Although the need for a multidisciplinary approach and the cooperation of governments and stakeholders regarding the prevention of violent extremism followed one key requirement of the *EU Counterterrorism Strategy* from 2005, van Ginkel and Entenmann pointed out, that not all EU member states have adopted comprehensive strategies that include preventive measures (Van Ginkel, Bibi, and Eva Entenmann, Eva, ‘The Foreign


39 Ibid.

40 Ibid.


43 Council of European Union 2020, p. 12.

44 Ibid., pp. 2ff.


46 Ibid.

47 Ibid., p. 5.

48 Ibid., p. 10.


51 Ibid.

52 Ibid., p. 20; p. 22.


55 See van Ginkel and Entenmann 2016.


58 Ibid., p. 31.

59 Ibid.


62 Europol 2020, p. 22.
63 Ibid., p. 61.
65 Dechesne and Paton 2020, p. 5.
66 Ibid.
70 Ibid., p. 85.
71 Ibid., p. 84.
72 The Pyramid Prevention model focuses on prevention measures for the well-being of people in a broad social context society (Level 0: Broad, societal context: political, social, cultural, ecological; Level 1: Improvement of the living environment and Level 2: General prevention) on the one hand. On the other hand, it consists of “urgent, problem-oriented immediate preventive measures (Level 3: Specific prevention and Level 4: Tackling the problem).” - Kudlacek et al. 2017, pp. 28ff.
75 Ibid., p. 27.
76 For more information see: https://ec.europa.eu/home-affairs/node/7447_en
78 Ibid.
80 Ibid., pp. 897ff.
83 Cf. Ellis, B. Heidi, et al., ‘Relation of Psychosocial Factors to Diverse Behaviors and Attitudes among Somali Refugees,’ Am J Orthopsychiatry, 86, 2016, pp. 393-408.


S.A.V.E. Belgium. Available at: https://savebelgium.org./.


Ibid.

Ibid., p. 23; p.41.


Ibid., p. 83; p. 85; p. 87.

Ibid., p. 38.

Ibid., p. 61.

Ibid., p. 68.

Ibid., p. 67.


Ibid., pp. 39f.


Ibid.

See Bertelsen 2015.
112 Ibid.
113 Ibid.
114 See Bertelsen 2015.
115 See Danish Government 2014.
118 Ibid.
121 Ibid.
122 See Bertelsen 2015.
124 See Gielen 2014.
131 Politiets Efterretningsstjenneste (PET), ‘The Centre for Prevention,’ PET. Available at: https://www.pet.dk/English/The%20Preventive%20Security%20Department/The%20Centre%20for%20Prevention.aspx.
132 Forebyggelse af ekstremisme og radikalisering (VINK). Available at: https://vink.kk.dk/.


Ibid.

Ibid., p. 20; p. 22.

Europol 2020, p. 85.

Ibid., p. 84; p. 37; p. 27.

Ibid., p. 37.

Ibid., p. 87; p. 26.

Ibid., p. 13; p. 35.

Ibid., p. 27.

Ibid., p. 29.


Ibid., p. 68.

Ibid., p. 73.

Ibid., p. 76.

Ibid., p. 66.

Ibid., p. 61.

Cf. Hecker, Marc, ‘137 shades of terrorism. France’s jihadists face justice’ (*137 nuances de terrorisme. Les djihadistes de France face à la justice*) *Focus stratégique*, n° 79, April 2018. Available at: https://www.ifri.org/fr/publications/etudes-de-lifri/focus-strategique/137-nuances-de-terrorisme-djihadistes-de-france-face.


See Brisard et al. 2018.

Global Counterterrorism Forum (GCTF), ‘*Initiative visant à interrompre le processus de radicalisation qui mène à la violence. Plan d’action pour l’identification et la lutte contre les recruteurs et les facilitateurs des terroristes*’ [Initiative aimed at interrupting the process of radicalization which leads to violence. Action Plan to Identify and Combat Terrorist Recruiters and Facilitators] GCTF, 2016, p. 3.


Sèze 2019a, p. 96; p. 89.


See Kepel 2012 and2015.

See Kepel 2015.


See Roy 2006.


L’Association Artemis. Available at: https://www.association-artemis.com/.

Plateforme d’harmonisation, de recoupement et d’orientation des signalements (PHAROS). Available at: https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action.

Stop Djihadisme. Available at: http://www.stop-djihadisme.gouv.fr

Kudlacek et al. 2017, p. 41.

Ibid., p. 42.

Europol 2020, p. 40.


Ibid., p. 20.

Europol 2020, p. 25.

Ibid., p. 26f.

Ibid.

Ibid., p. 32.

Ibid., p. 19.

Ibid., p. 54.

Ibid., p. 69.

Ibid., p. 14; p. 68.

Ibid., p. 62.

Ibid., p. 59f.

Ibid., p. 60.

Ibid., p. 23.

Kudlacek et al. 2017, p. 66.

Europol 2020, p. 59.

Ibid., p. 40.

Ibid., p. 42.

Kudlacek et al. 2017, p. 60.

Cf. BMFSFJ, Leitlinie Förderung von Demokratiezentren zur landesweiten Koordinierung und Vernetzung sowie von Mobiler, Opfer- und Ausstiegsberatung.[Guideline for the promotion of democracy centres for country-wide coordination and networking as well as


See Younes 2018.


See Younes 2018.


Kudlacek et al. 2017, p. 69.


Ibid., p. 20.

Ibid., p. 24.

Ibid., p. 25.

Europol 2020, p. 12.

Ibid., p. 18.


Ibid.


Aked 2020, p.8.

Aked 2020, p. 8.


The Scottish equivalent to the Channel Programme that is applied on pre-radicals in England as well as in Wales is named the Prevent Professional Concerns Programme.


See Nye, Catrin, ‘The man who is being deradicalised,’ BBC News, 1 September 2015. Available at: https://www.bbc.co.uk/news/uk-34073367.

See Home Office 2019c.

Aked 2020, p. 6.
253 Ibid., p. 9; For assessments on this research-field from disciplines other than the therapeutic field, see for instance, Corner, Emily, and Gill, Paul, ‘Is there a nexus between terrorist involvement and mental health in the age of the Islamic State?’ *CTC Sentinel*, 10(1), 2017, pp. 1-10.
254 Ibid., p. 7.
255 Ibid.
256 Aked 2020, p. 7.
257 Ibid.
260 Aked 2020, p. 25; p. 68.
261 Ibid., p. 7.
262 Ibid., p. 8.
268 See Qureshi 2016.
271 Several examples of Muslims being portrayed as “enemies” of UK are for instance discussed in: Evans, Jonathan, *Intelligence, Counter-Terrorism and Trust. Address to the Society of Editors*, Security Service M15, 5 November 2007. Available at:

282 See Muslim Council of Britain (2015 and 2016), op. cit.; See Prevent Watch, ‘What is Prevent?’ Prevent Watch. Available at: https://www.preventwatch.org/joint-statement-on-prevent/.


287 https://www.activechangefoundation.org/.


289 Moaveni 2019, p. 92. Since 2019, Hanif Qadir is working as a consultant for The International Institute for Justice and Rule of Law (IIJ) for the rehabilitation and reintegration of terrorist fighters. He has strongly criticized governmental plans to save money by closing Youth Centres, where vulnerable young adults can be prevented from being radicalized.

290 Active Change Foundation. Available at: https://www.activechangefoundation.org/.
291 Club de Madrid, n. y., p. 9, op. cit.
292 Imamsonline. Available at: http://imamsonline.com/
293 See BBC Asian Network, ‘Interview with Ahmed Patel, 7/7 bomber’s former brother-in-law: “There were no signs”,’ BBC, 9 September 2016. Available at: https://www.bbc.co.uk/sounds/play/p047bv99.
296 Cf. DERAD (European project towards the prevention of the escalation of radicalization in prisons). Available at: https://www.agenformedia.com/international-projects/derad.
297 Cf. HERMES. Available at: https://www.traininghermes.eu.
299 See Moaveni 2019.
300 Moaveni 2019, p. 271.
301 Ibid., p.151.
Cf. Hanif Qadir and his former approach ‘Not born radical’; Available at: https://www.activechangefoundation.org; cf. Käsehage 2018, pp. 477f.

Ibid., p. 468.

This approach supports a diverse range of religions, cultures and life-models that are living together in harmony. See, for instance: Bérubé, Maxime, Implementing Montreal’s Centre for the prevention of radicalization leading to violence: Insights from the 2015 TSAS Summer Academy. Université de Montréal, October 2015.

The Good Lives Model assumes that the main aim of an individual is to live a good life without major problems. Therefore, every society should enable citizens to achieve this and thereby avoid being attracted to negative goals. See Marsden 2016, op cit.


Yasmeen 2005, p. 38.


Council of European Union 2020, p. 16.

Ibid., p. 10.

Käsehage 2018, pp. 478f.


Käsehage 2018, pp. 479f.

See Koehler & Ehrt (2018), op. cit.


Gill, Horgan, and Deckert 2014, p. 429.

Koehler 2015a, p. 133; See Horgan 2008 and 2009.

Ibid. This term indicates a broader approach of the study in terms of patients affected by physical or mental health issues in an appropriate relation to its appearance.


BBC Asian Network, ‘Interview with Ahmed Patel, 7/7 bomber’s former brother-in-law: ‘There were no signs’,’ BBC, 9 September 2016. Available at: https://www.bbc.co.uk/sounds/play/p047bv99.


Bérubé, Maxime, Implementing Montreal’s Centre for the prevention of radicalization leading to violence: Insights from the 2015 TSAS Summer Academy. Université de Montréal, October 2015.


Dantschke, Claudia, ‘Lasst euch nicht radikalisieren! ‘Salafismus in Deutschland” [‘Don’t allow yourself to be radicalized!] Salafism in Germany’]; in: Thorsten Gerald Schneider (ed.), *Salafismus in Deutschland, Ursprünge und Gefahren einer islamisch-fundamentalistischen Bewegung* [Salafism in Germany, Origins and Dangers of an Islamic-fundamentalist Movement]. Bielefeld: Transcript, 2014, pp. 171-186.


Department Onderwijs and Vorming [Ministry of Education and Training], *Handvattn voor de Preventie, Aanpak en Omgang met Radicaliseren & Polariseren Binnen Hoger Onderwijs en Volwassenesonderwijs* [Guidance for Prevention, Approach and Handling


Ellis, B. Heidi, et al., ‘Relation of Psychosocial Factors to Diverse Behaviors and Attitudes among Somali Refugees,’ Am J Orthopsychiatry, 86, 2016, pp. 393-408.


Fischbacher-Smith, Denis, ‘Framing the UK’s counter-terrorist policy within the context of a wicked problem,’ Public Money & Management, 36(6), 2016, pp. 399-408.


Forebygelse af ekstremisme og radikalisering (Prevention of Extremism and Radicalization, or VINK). Available at: https://vink.kk.dk/.


Global Counterterrorism Forum (GCTF), ‘Initiative visant à interrompre le processus de radicalisation qui mène à la violence. Le rôle des familles dans la prévention et la lutte contre l’extrémisme violent: recommandations stratégiques et options programmatiques,’


Hecker, Marc, ‘137 nuances de terrorisme. Les djihadistes de France face à la justice’ [‘137 shades of terrorism. France’s jihadists face justice’]. Focus stratégique, no 79, April 2018. Available at: https://www.ifri.org/fr/publications/etudes-de-lifri/focus-strategique/137-nuances-de-terrorisme-djihadistes-de-france-face.


Home Office, ‘Individuals referred to and supported through the Prevent programme, England and Wales, April 2018 to March 2019,’ Home Office, 19 December 2019. Available at:


Hymas, Charles, ‘Free counter-terrorism training offered online by police to all Britons in run-up to Christmas,’ The Telegraph, 8 December 2019. Available at: https://www.telegraph.co.uk/news/2019/12/08/free-counter-terrorism-training-offered-online-police-britons/.


Kenney, Michael, The Islamic State in Britain. Radicalization and Resilience in an Activist Network. Cambridge: Cambridge University Press. 2018


Khan, Khalida, ‘Preventing Violent Extremism (PVE) & PREVENT: A Response from the Muslim Community,’ *AN NISA Society*, 2009.


Malthaner, Stefan, and Waldmann, Peter, Radikale Milieus, Das soziale Umfeld terroristischer Gruppen. [Radical milieus: The social environment of terrorist groups], Frankfurt am Main: Campus, 2012.


Martinez, Magdalena, ‘Loss of Identity, Radicalization, and Terrorism. Case Studies in France and Belgium,’ (Master’s Thesis). San Francisco: University of San Francisco,
California, 2016. Available at: https://repository.usfca.edu/thes/195/?utm_source=repository.usfca.edu%2Fthes%2F195&utm_medium=PDF&utm_campaign=PDFCoverPages.


McLaughlin, Gilbert, ‘Penser la radicalisation politique en France,’ [Thinking about political radicalisation in France]. Études internationales, 50(1), Spring 2019, pp. 147-160.


Nye, Catrin, ‘The man who is being deradicalized,’ BBC News, 1 September 2015. Available at: https://www.bbc.co.uk/news/uk-34073367.


Perry, Barbara and Scrivens, Ryan, ‘Right Wing Extremism in Canada: An Environmental Scan,’ Public Safety Canada, September 2016.


Plateforme d’harmonisation, de recoupement et d’orientation des signalements (Platform for Harmonization, Analysis, Cross-PHAROS (Checking and Orientation of Reports). Available at: https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action.

Politietets Efterretningsstjeneste [PET - Danish Security and Intelligence Service], ‘The Centre for Prevention,’ PET. Available at: https://www.pet.dk/English/The%20Preventive%20Security%20Department/The%20Centre%20for%20Prevention.aspx.


Pulinx, Rienhilde, and van Avermaet, Piet, ‘Integration in Flanders, Citizenship as Achievement,’ J Lang Polit, 14, 2015, pp. 335-358.


Available at: https://www.files.ethz.ch/isn/153962/CGCC_EvaluatingTerrorismPrevention.pdf.
S.A.V.E. Belgium. Available at: https://savebelgium.org/.


Thomson, David, Les Revenants, ils étaient partis faire le jihad, ils sont de retour en France. [The Revenants: They had gone to jihad, they are back in France]. Paris: Seuil, 2016.


Van der Veen, Jaap, ‘How Preventive Counter-Radicalization Interventions Can Stigmatize Their Target Groups,’ (Master’s thesis), University of Amsterdam, 2017.


Witteveen, Wouter, ‘Preventie van radicalisering is geen kwestie van indammen maar van voorkomen,’ [Preventing radicalization is not a matter of containment, but of prevention] *Sociale Vraagstukken*, 27 March 2017. Available at: https://www.socialevraagstukken.nl/preventie-van-radicalisering-is-geen-kwestie-van-indammen-maar-van-voorkomen/.


Web-based Resources

Centre for the Prevention of Radicalization leading to Violence (CPRLV)
Available at: https://info-radical.org/en/

Combating Terrorism Center (CTC) at Westpoint
Available at: https://ctc.usma.edu/

Council of Europe (HELP Radicalisation Prevention)
Available at: https://www.coe.int/en/web/help/help-radicalisation-prevention1

Counter Terrorism Group (CTG)
Available at: https://www.counterterrorismgroup.com/

DERAD (European project towards the prevention of the escalation of radicalization in the prison)
Available at: https://www.agenformedia.com/international-projects/derad

FHAR (Hybrid Training with Religious Community Leaders)
Available at:

German Congress on Crime Prevention (GCOP)
Available at: https://www.gcop.org/

Global Counterterrorism Forum (GCTF)
Available at: https://www.thegetf.org/HERMES
Also available at: https://www.traininghermes.eu

International Crisis Group (ICG)
Available at : https://www.crisisgroup.org

International Centre for Counter-Terrorism - The Hague (ICCT)
Available at: https://icct.nl/

International Centre for the Study of Radicalization and Political Violence (ICRS)
Available at: https://icsr.info

PHAROS Available at: https://www.internet-signalement.gouv.fr/PortailWeb/planets/
Accueil! input. action

(European) Radicalisation Awareness Network (RAN) Available at:

START (Global Terrorism Database) Available at: https://www.start.umd.edu/gtd

Youth Counselling Against Radicalisation (YCARE) Available at: https://www.ycare.eu
Chapter 12

Prevention of Radicalization on Social Media and the Internet

Sara Zeiger and Joseph Gyte

In the age of selfies, snaps, likes and shares, the internet and social media have transformed the way in which people communicate. In early 2019, global internet penetration reached 57%, or 4.4 billion users, and the overall number of mobile social media users reached 42%, or 3.2 billion people.¹ This means that people are able to share ideas, communicate and interact more rapidly than ever before, including with audiences on the other side of the world. Terrorist groups have certainly leveraged these new mechanisms and platforms for communicating amongst themselves and to potential recruits. For example, the Islamic State of Iraq and al-Sham (ISIS) has been known for producing sleek videos circulated on YouTube and Twitter, and has mastered new and emerging technologies and social media platforms, such as Telegram; all to promote its messages and recruit new members in cyberspace.

This chapter focuses on the prevention of radicalization on social media and the internet in this digital age. It first reviews the relevant methods and approaches that terrorists employ to spread their propaganda and recruit online. Subsequently, it looks at some of the more common and emerging prevention and preparedness strategies which address the online space. Besides reviewing the theoretical foundations to prevent radicalization on social media and the internet, this chapter will also draw upon specific examples, predominantly from three regions: Europe, Southeast Asia and East Africa, to illustrate what some countries are doing to tackle the problem of online radicalization.

Keywords: radicalization, violent extremism, prevention, online, internet, social media, propaganda, counter narratives.
Contemporary terrorist groups are the first generation whose members have grown up with access to the internet and social media. It should not be surprising, therefore, that these online platforms play a critical role in their approach to radicalizing and recruiting vulnerable individuals. In fact, social media and the internet have become increasingly useful facilitators of the promotion, incitement, intimidation, and radicalization of a much wider and previously unreachable audience.

Many terrorist organizations achieved great success through this approach. Online technologies, including social media, have many benefits—which are often leveraged by terrorist groups. They are able to reach audiences globally immediately, yet also tailor their messages to fit with different target audiences at the local level. They are able to develop rich content for the mass market, and still recruit individuals with privacy protections. Indeed, terrorist groups have proven to be innovative and adaptable, partially exploiting modern social communication systems and leveraging modern tools to achieve their aims.

Actors responsible for the prevention of online radicalization and recruitment face significant challenges. Most online platforms are owned and controlled by private companies, oftentimes under a different jurisdiction to that of the terrorists’ location. Additionally, many terrorist groups have internally emphasized the importance of these social media platforms for recruitment and in order to develop high-quality, attractive propaganda, as well as effective marketing strategies for content dissemination. Furthermore, the sheer volume of terrorist propaganda published on an assortment of platforms has made it particularly challenging to contain their online presence.

Despite this, there are a number of potential legislative and policy measures to address this challenge, including: blocking online content and access; filtering and removing content; empowering online communities to counter the narratives of violent extremism and terrorism; the promoting positive and alternative messages; as well as building digital resilience and media literacy.

In this regard, through the use of in-depth desk research, this chapter will first outline some of the methods used by terrorist groups for radicalization on social media and the internet. Subsequently, it will address prevention strategies that are being—and possibly could be—implemented by the private and public sectors.

Terrorists’ Methods for Radicalization on Social Media and the Internet

Due to the evolving nature and the vast variety of online platforms, as well as the breadth of exploitative techniques used, this section takes a broad approach when examining terrorists’ methods, focusing on major platforms available at the time of writing, but noting the likelihood of other platforms being used. The methods presented should not be seen to be the only approaches employed, but rather a limited sample to provide a basic framework for understanding. In this regard, this section addresses how terrorist organizations have used social media and the internet to: adjust their structures and aims; enhance the quality of their propaganda materials; disseminate their messages to wider audiences; and recruit through more secure messaging platforms and leveraging new technologies. Select case studies will be utilized throughout for practical clarification of how terrorists are interacting with, radicalizing, and recruiting, vulnerable individuals online.

Structures, Dynamics and Aims of Terrorist Organizations

Terrorist organizations are dynamic systems that adapt and evolve over time. Traditionally, terrorist organizations were thought to have a centralized, hierarchical structure in which the leaders at the top controlled the operations of the entire organization. These traditional
structures would often have a well-defined chain of command and control, with great specialization of functions for individuals and branches. This enabled hierarchical terrorist organizations to effectively maintain consistency in their disseminated message through specific individuals, but also increased the risk of interruption if the individual and/or unit was compromised.4

In recent years, social media and the internet have accelerated the speed, increased the complexity, and reduced the cost of sharing information. This has, in turn, supported the process of many terrorist organizations to reorganize themselves into a network style structure and enhanced the capacity of each cell and individual to operate more independently, especially for the dissemination of the organization’s messages. This reorganization has provided them with greater flexibility, responsiveness, resilience, and outreach.5 As a result, wider terrorist networks can remain operational, even if one or more cells are severely damaged or dismantled.6 For example, after 9/11, Al-Qaeda suffered from increased pressures, lost training camps in Afghanistan, and many of the pre-9/11 senior leadership had been killed or captured. Therefore, in order for Al-Qaeda to remain relevant, they had to shift their approach toward inspiring and guiding other violent extremist groups, even if only through loose connections. Abu Musab al-Suri was one of the principal instigators for this shift in structure and strategy, and the internet was exploited as a means to facilitate this shift. This change in approach resulted in significant global impacts, as witnessed by the formation of local affiliated groups which conducted terrorist attacks in Bali, London, and Madrid.7

Now, modern terrorist networks typically consist of widely distributed, smaller cells who communicate and coordinate their campaigns in an interweaving fashion.8 Relationships are often temporary and vary in intensity, depending on the task at hand. This has facilitated groups to develop not only wider internal connections, but external relationships as well, which tend to be based on shared norms, values, and mutual respect, rather than formed through formal bureaucratic structures.9

These characteristics of a networked approach were exemplified by the Charlie Hebdo attack, in Paris, France, in January 2015. One of the terrorists involved, Amedy Coulibaly, released a video stating that the attacks were carried out in the name of ISIS. However, the poor quality of the video suggested that this attack was not directly tied to ISIS’ central media hub, al-Hayat Media; rather this was likely a smaller cell coordinating independently.10 It was also reported that the other two terrorists involved, the Kouachi brothers, received $20,000 from Al-Qaeda in the Arabian Peninsula (AQAP), which highlights the increasing role of ad hoc external coalitions, caused by the networks communicating autonomously.11

In addition, the information revolution has also helped terrorist groups to move away from that of a traditional war model and move towards a new mode of conflict at societal levels. While terrorist organizations have always put effort into conducting psychological operations, they now have the capacity to conduct information operations on a much grander scale. Understanding the importance of knowledge and soft power, networked terrorists leverage social media and the internet for brand management12 and propaganda, with the aim to influence public opinion and attract new recruits. Previously, terrorist organizations relied on traditional media, such as television, radio, leaflets, print, and in-person conversations to conduct their psychological operations. However, the internet and social media now provide an opportunity for terrorist organizations to increase the volume and diversity of disseminated messages, including a localized approach by individual cells. Hence, while terrorist organizations have always recognized how conflicts revolve around knowledge and information, they now have greater control over the information available, and consequently place greater emphasis on information operations which “aim to attract or disorient rather than coerce, and that affect how secure a society, a military, or other actor feels about its knowledge of itself and of its adversaries.”13
In this regard, whilst terrorist propaganda will often depict violent behaviour, such as beheadings, with the intention of coercion or to encourage that such violence be imitated by others, some propaganda now also focuses on brand management, through the portrayal of a narrative that aims to attract individuals to their cause. Such narratives can take two approaches (or a combination of both): that which focuses on the personal incentives for joining the group (pull factors) and that which emphasizes or exaggerates the negative social, political, and/or economic conditions of the target population (push factors), thereby contributing towards a fertile environment for recruitment.

Moreover, the global reach of these online platforms has allowed terrorist networks to merge and spread across national boundaries, cultures, and languages. This has been manifesting itself through the increasing occurrence of global coalitions of previously separate terrorist organizations. Most noteworthy was the pledging of allegiance (bayat), to Abu Bakr al-Baghdadi, the leader of ISIS. In light of geographic and security restrictions, which prevented oaths of allegiances being given in person, social media provided an alternative approach. In Southeast Asia, for example, several terrorist groups in the Philippines and Indonesia, including Maute, Abu Sayyaf, Katibat Ansar al Sharia, and Mujahidin Indonesian Timor, all pledged their allegiances via online videos. In response, acceptance of the pledges was also released through online video.

These adaptations, interactions, and behaviours highlight how the internet and social media have enabled terrorist groups to communicate, coalesce, and operate as global networks, while simultaneously providing greater freedoms for individual members and cells to coordinate, reach, and recruit target populations. Centralized messages can independently be adapted to a narrative that resonates in a localized context, in order to address the push and pull factors of the local population. ISIS, for example, has established media units in multiple regions, which are capable of producing sophisticated and locally contextualized propaganda materials, in the language and culture of the target population.

Videos, Images, and Magazines: Propaganda

In parallel to social media and the internet enabling terrorist organizations to operate globally and distribute controlled propaganda, the wide diversity and availability of digital equipment, such as high-definition (HD) cameras and editing software, has also empowered terrorist organizations to produce propaganda of a quality similar to that of Hollywood movie professionals and those of the best marketing firms. In fact, high quality propaganda has become increasingly important for a terrorist organization’s branding strategy. The use of attractive digital media and novel methods contributes to the amplification of their brand, and has become an approach taken by numerous terrorist groups other than ISIS. The logic behind it is clear: in the battle for hearts and minds, they need to stand out and inspire individuals so as to secure recruits in an increasingly competitive environment.

When propaganda can attract viewers as well as present a strong narrative that addresses the push and pull factors of local communities, it is likely to impact the radicalization process of vulnerable individuals. For example, Al-Hayat Media has produced many HD videos in the native languages of Europe, such as French and English, which targeted potential recruits and sympathizers by depicting life within ISIS territory as spiritually fulfilling, while at the same time declaring the European states to be immoral and unlawful. The production and distribution of such well-designed videos addresses the feelings of dissatisfaction present among parts of the European (diaspora) youth and offers a positive alternative. Such videos have played a significant role in the radicalization process of many young European Muslims and converts to Islam. Another modern example of high-quality propaganda is that of the video game Salil al-Sawarem (The Clanging of Swords): a “first-person shooter” game that was modelled on the
popular Grand Theft Auto franchise, and aimed to gain publicity for and draw attention to ISIS. Trailers for the game were released on multiple websites and platforms across the internet, most notably YouTube, which at the time of the game’s release in 2014, had 3.5 billion views a month on its gaming channels alone. The use of cinematic productions and social media, and building on the engaging appeal of a videogame demonstrated the terrorists’ tactic of exploiting popular culture as a means of enhancing the virality of their propaganda, as well showcasing their approach to reach the target audience—in this case game-loving youth.

In this way, these types of sophisticated communications can easily go viral. The modern appearance assists with translating the terrorists’ violence into a language that is understandable for the average young viewer, thereby increasing the psychological impact on the target audience.

In addition to games, videos, and images, several terrorist groups also publish online magazines, and these publications appear to play an important role in online radicalization. The accessibility and popularity of sleek online magazines has reportedly contributed towards the successful enlargement of several terrorist organizations, including ISIS, through their magazines Dabiq and Rumiyah, Al-Qaeda via Inspire, and Al-Shabaab through Gaidi Mtaani.

Digital magazines provide their readers with a wide array of narratives in a single, well-presented package. Through the use of collective stories, individual stories, and event stories, terrorist magazines attempt to construct a wider narrative that resonates with their readers. In this regard, magazines can combine a multitude of various approaches. The inclusion of images that show fighters in militarized clothing has been shown to attract individuals to violence. Additionally, emphasis on masculinity and bravery has been found to appeal to individuals who desire excitement and are attracted to thrill seeking. The inclusion of other styles, such as the use of religious quotes, the presentation of members as heroic, their deaths as a sacrifice, and the portrayal of a common enemy, all have their own meanings, appeal to diverse readers, and lead towards a philosophical discussion and common ground.

A secondary use of digital magazines is that the purpose cannot just be to inspire readers, but also to supply them with technical instructions on how to carry out violent acts as lone actors, or provide them with advice on joining the terrorist group. The Boston Marathon bombing in 2013 was one such case. The brothers Tamerlan and Dzhokhar Tsarnaev, had read Al-Qaeda’s Inspire magazine online, among other online propaganda, and claimed to have learnt how to make the bomb from an article in the magazine’s first issue, titled How to Make a Bomb in Your Mother’s Kitchen.

The ability of terrorist organizations to produce inspiring, high quality propaganda that can be shared on social media and the internet has been of critical importance for their brand management and their approach to radicalization. In fact, social networking sites, such as Facebook, Twitter and YouTube, have become the modern-day tools that help to disseminate even the oldest of messages in a modern and relatable format.

Social Networking Sites: Offering an Open Invitation to Everyone

The rise of social networking sites has enabled individuals and terrorist organizations alike to share information with large audiences instantaneously, irrespective of their geographic distance. Terrorists and their followers too are now able to share materials which can travel outside of their own social circles and reach populations that were previously inaccessible.

The first terrorist to fully exploit this potential to an English-speaking audience was Anwar al-Awlaki, a US-born prominent Imam in AQAP dubbed the “bin Laden of the Internet.” He realized that despite the quality in which it was produced, online propaganda was not reaching as wide an audience as possible. In response, he pioneered the use of social networking sites to enlarge its scope, creating his own blog, Facebook page, and YouTube channel where he
frequently shared his increasingly sophisticated videos and the online magazine *Inspire*.\textsuperscript{36} Since then, terrorist organizations have specifically sought out Information Technology (IT) experts and skilled online marketers to lead their online propaganda campaigns,\textsuperscript{37} which are now spread primarily via social networking sites.\textsuperscript{38}

Most major social networking sites have instituted highly publicized and broad responses in an attempt to curtail the violent extremist content published on their platforms in recent years.\textsuperscript{39} Unfortunately though, these platforms continue to be used by ideologues and recruiters, who remain adept at sharing propaganda and attracting followers.\textsuperscript{40} In fact, an analysis of 1,000 pro-ISIS Facebook profiles from across 96 countries in 2018 found that the group’s Facebook networks are still growing globally, despite efforts to take down new accounts as they emerge and are identified.\textsuperscript{41}

These sites, which have become instrumental for the sharing of high-quality propaganda materials, have also become instruments for personal storytelling and for providing platforms for terrorists to share their experiences. Moreover, through the avoidance of posts that contain images and videos that could be censored by the host platforms, many of these stories remain online. These intriguing and personal narratives promote viral imitation, and have become a central feature in the recruitment process, particularly as a means to inspire those in pursuit of a new identity.\textsuperscript{42}

An example of one such case is that of Siti Khadijah alias Ummu Sabrina, an Indonesian woman who managed Facebook pages for Kabar Dunia Islam (KDI), a media wing of ISIS based in Indonesia. She became well-known after posting her experience of traveling to Syria with her husband and their four children, which she published on Facebook, in June 2014. Following this, she regularly posted about her life in Syria, promoting the terrorist group’s positive narrative of a monthly stipend, free schooling and healthcare, and how well her family had been treated. In response, her Facebook page was inundated with questions from Indonesians wanting to know how they too could travel to Syria. One Indonesian, for example, who went by the Facebook name Shabran Yaa Nafsi, was inspired by Siti Khadijah’s story and travelled with his family in 2015 to Syria, where he was later killed.\textsuperscript{43}

A similar example from a different geographical location was that of Aqsa Mahmood, a Scottish woman who travelled to the conflict zone in Syria and Iraq in 2013, when she was 19 years old. British authorities suspected that her use of social media, including Twitter and Tumblr, had contributed towards the radicalization and recruitment of a number of British teenagers. Similar to Siti Khadijah, Mahmood used social media to promote positive images of life under ISIS, and would frequently post propaganda publications, poems, religious verses, quotes by prominent extremists, and advice on how to travel to Syria.\textsuperscript{44} These messages reached a wide audience, and encouraged other Westerners to travel to Syria and join Mahmood in her new life.

In addition to personal narratives, social networking sites have been used to control the narratives surrounding an event. During the Westgate terrorist attack in Kenya in 2013, Al-Shabaab made extensive use of Twitter for this purpose. An analysis of 556 tweets posted by Al-Shabaab throughout the attack found that the aim of these tweets was to control the narrative and retain the audience while they were trending online.\textsuperscript{45} This approach, which has also been used by other terrorist groups, is known as “Hijacking a Twitter Storm”: the posting of propaganda with a trending hashtag in order to take advantage of the huge traffic to greatly increase visibility.\textsuperscript{46} These examples, among others, all point in a similar direction; radicalization and recruitment through social networking sites are especially well-supported by personal narratives, stories, and first-hand reports, which are popularized and become viral. This in turn, then causes a chain reaction of imitations, particularly among those seeking to find their own identity.\textsuperscript{47}
As well as using mainstream social media, such as those mentioned already, it should also be noted that terrorist groups use a wide range of various other social networking sites, including Flickr, Vimeo, Instagram, and SoundCloud, as well as their own blogs and websites, and file upload sites, such as Justpaste.it.\(^48\) Having a larger volume of content online not only assures visibility, but simultaneously grabs the attention of the mass media (news outlets), thereby propagating the exposure to the propaganda further. This style of increasing conspicuousness helps terrorist organizations to seem more powerful than they actually may be, a phenomenon referred to as “force multiplication.”\(^49\) which can have significant results. By increasing their communications, even a small group can create an exaggerated representation of the group’s size, strength, and support in the community.\(^50\) This, in turn, can then also directly affect reality: simply projecting the appearance of possessing many followers has been shown to increase the number of real followers.\(^51\)

Furthermore, social networking sites provide support for the promotion of lone actors’ narratives as well. For example, on 15 March 2019, 51 people were killed during terrorist attacks on two mosques in Christchurch, New Zealand.\(^52\) The day before the attacks, the perpetrator, a right-wing violent extremist, posted his manifesto on Twitter and although his account was suspended after the attack, the 74-page anti-immigrant manifesto went viral before suspension.\(^53\) Additionally, the perpetrator live-streamed the attacks through Facebook Live, via a head-mounted camera. Again, while the attacker’s Facebook account was later removed, he streamed the attack for 17 minutes,\(^54\) providing more exposure to his manifesto and narrative. In fact, this was further exacerbated by the copying and sharing of the video. In the first 24 hours after the attack, Facebook removed 1.5 million copies of the video and continued to find 800 visually distinct videos related to the original in the following days.\(^55\) This clearly demonstrates how these platforms have provided extended scope for terrorist propaganda to reach a far wider audience than previously possible.

In addition to the messages and materials, the online accounts of violent extremists and terrorists are also frequently identified and deleted. However, these accounts are often reinstated multiple times after being removed, under different names or locations, allowing them to remain relatively unaffected by the implemented counter measures. For example, while ISIS has a limited number of central actors who are primarily responsible for online propaganda, no single individual account serves as an irreplaceable connection.\(^56\) Moreover, as previously mentioned, terrorist propaganda can remain on a platform for long periods of time.\(^57\) Such was the case of Ahmad Qadan, based in Sweden, who, through his Facebook profile, promoted ISIS and posted invitations such as “Contact me to support your brothers at the front,” which remained on his Facebook profile from May 2013 to June 2015, until it was removed from the platform.\(^58\) Qadan’s status highlights another key aspect of social networking sites: direct connections. As well as the use of these platforms for spreading sophisticated propaganda to wide audiences, and presenting personal narratives, they are also valuable to terrorist organizations for identifying and connecting with specific individuals who may be susceptible to recruitment.\(^59\) However, having more explicit conversations with a potential recruit or fellow terrorist on a social networking site can leave these individuals more open to police monitoring. Therefore, once a recruiter identifies a potential recruit, they will often recommend moving over to a more secure platform to continue communications.\(^60\) In other words, social networking sites are primarily used for disseminating propaganda and for radicalization purposes, e.g. by planting the seeds of dissatisfaction or offering alternative identities, which may not have been considered otherwise. On the other hand, private messaging channels are more often utilized for individual recruitment and coordination.
Messaging, Broadcasting and Channels

As the previous section has shown, online platforms have the potential to significantly influence the radicalization and recruitment process. Once a vulnerable individual who may be susceptible to recruitment is identified, the recruiter will often guide the person to a more secure means of communication: either a one-to-one messaging application or a forum/channel (such as 4chan, 8chan or 8kun) with like-minded individuals. Many recruiters now rely on unregulated and unpolicied mobile messaging applications such as WhatsApp, Telegram and Kik, in order to deepen the contact with a potential recruit. This highlights the importance of different types of social media platforms and different online media tools in the recruitment process. While some platforms and tools are more effective at spreading violent extremist messages to a broader audience, others aid the recruiter in guiding an individual towards one-to-one and eventually face-to-face interactions.

Encryption technology has been used by some terrorist organizations for the last couple of decades, for example, Pretty Good Privacy (PGP) was first created in the mid-1990s and Al-Qaeda’s Inspire magazine would share its public-key, so that anyone could send an encrypted message to the publishers of the magazine. However, most forms of encryption were primarily only available for higher ranking terrorists in an organization and mainly used for the coordination of attacks. Now, almost all terrorists and their recruiters make use of encryption technologies. In fact, terrorists now have access to a much larger market of encrypted communication options. For example, Skype, the internet-based telephone system, and one of today’s largest online communication tools, is encrypted, allowing terrorists to speak in real time without a major risk of anybody discovering the content of their conversations. Encrypted emails, like those offered by bitmessage.ch, also provide sophisticated methods for secure communications. Often not only is the original message encrypted but it is also sent to hundreds of other randomly selected accounts, making it virtually impossible to decipher who is the intended recipient who possesses the encryption key.

Telegram, a free messaging application which allows its users to instantly send text messages, voice messages, pictures, videos, and any file type, has become the application of choice for most modern terrorist organizations. This is because Telegram provides “secret chats” with end-to-end “military grade encryption,” which is not stored anywhere else but on the user’s phone, while not even being accessible by the platform provider. Additionally, the platform provides further security, such as passcode locking the application and self-destruct timers on messages after being read.

In Indonesia, the use of Telegram and other encrypted messaging services has reportedly contributed to the reinforcement of group solidarity, as members have been able to increase the sharing of information in a secure way. Bahrun Naim, who was one of ISIS’ top Indonesian propaganda distributors, used Telegram extensively. For example, in June 2015, Naim contacted a former friend, alias Ibad, via Facebook and connected him to his Telegram. They subsequently began to communicate about Ibad traveling to Syria via the encrypted service.

Although encryption offers terrorists security of content, it does not necessarily keep them anonymous. The so called “dark internet” service providers and anonymous operating systems can often be used in unison with these encryption communications in order to further ensure anonymity. The popular and often free means for achieving anonymity is “Virtual Private Networks” (VPN). These VPNs conceal a user’s IP address and can make it appear in one or multiple countries, preventing, or at least slowing down, the security agencies’ abilities to trace the source. The Onion Routing (TOR), originally created for the US Navy, is one such anonymous browser which utilizes such techniques. These easy and often free forms of encryption and online anonymity have greatly impacted the recruitment process by allowing
terrorists not only to send messages and files instantaneously, but to remain hidden and secure whilst doing so.

**Leveraging Artificial Intelligence and Emerging Online Technologies**

Finally, it is worth mentioning that terrorist groups are beginning to explore the use of Artificial Intelligence (AI) in their online radicalization and recruitment strategies. In the example from Indonesia above, Bahrun Naim also established a bot (an online “robot” application or program that autonomously completes tasks by interacting with systems and users) for communicating with potential recruits. The bot would greet users with an automated message in Bahasa Indonesian and subsequently share propaganda messages and videos, such as interviews with militants, as well as guides for the fabrication of homemade explosives. Al-Shabaab’s news agency, Shahada, also used a bot on Telegram. The bot would send users a link to the most recent channel, which allows Shahada to remain in constant connection with its followers, even after an iteration of their channel had been suspended. There is also speculation that more sophisticated language tools could be leveraged by terrorist groups to generate new content. For example, in a 2019 study, researchers speculated that open source AI tools, such as GPT-2, could be used by malicious actors, including terrorist groups, to post auto-generated commentary on current events, overwhelm conversations on social media channels, or re-direct conversations online to match with their ideological views. The report did not find evidence that GPT-2 was being used by terrorist groups, but it also found that existing auto-detection technology was not always able to distinguish human-generated extremist content from GPT-2-generated extremist content. This means that if terrorist groups begin to leverage open-source AI tools, it will take a human, not a machine, to accurately detect auto-generated terrorist content based on new technology.

Changes in internet structure and emerging technologies are also starting to be used by terrorist groups to circumvent detection, and this is complicating abilities to detect and take down terrorist content online. For example, the increasing use of decentralized web (DWeb) models, instead of centralized servers, mean that content can be stored across multiple users and multiple servers where hosting - and therefore takedown - cannot be controlled by a single source. A switch to using DWeb services by a terrorist group like ISIS would essentially mean their propaganda would be almost impossible to eliminate from the internet. As another example, the alt-right’s expanding use of social networks such as Gab has raised some alarm bells with counterterrorism researchers. In this case, Gab’s browser extension Dissenter allows for contentious debate and commentary on news articles that is not visible to anyone that does not have that extension installed, thus meaning automatic content detection is not usable on this platform. As new online technologies emerge, terrorists’ use of these technologies is always a potential danger for further radicalization and recruitment strategies.

In summary, the internet and social media have been leveraged by terrorist organizations, which has also been correlated with a restructuring of organizations into local network cells that report globally but respond locally. Subsequently, terrorist groups have increased the sophistication of their propaganda materials and used social networking sites for dissemination. These platforms are also used to share personal and relatable messages that feed into their wider narrative. Essentially, social media and the internet have given terrorist organizations the means to effectively manage their brand both at a global and a local level. In addition, once a vulnerable individual is identified, encrypted messaging services can be used for the provision of specific information on how to carry out attacks or join the terrorist organization.

These methods of exploitation of social media and the internet pose considerable challenges for government authorities to prevent and counter online radicalization, either due to the sheer volume of online materials shared, the attractiveness of the narrative, or through high-end encryption software which makes it difficult to track. Moreover, new and emerging
online technologies, such as AI and DWeb, if appropriately leveraged by terrorist groups, have the potential to further complicate potential prevention efforts aimed at reducing radicalization and recruitment through online channels.

**Prevention Strategies for Radicalization on Social Media and the Internet**

Noting the elaborate techniques used by terrorist groups that were outlined in the previous section, this chapter will now turn to possible solutions for preventing and countering radicalization on social media and the internet. Drawing on a strategy proposed by Stevens and Neumann, this chapter will examine three broad areas of how prevention of radicalization online might be possible: preventing the spread of terrorist content online (deterring producers); empowering online communities to counter the narratives of violent extremism and terrorism online and promote positive and alternative messages; and building digital resilience and media literacy (reducing the appeal).

**Preventing the Spread of Terrorist Content Online**

The first strategy for preventing radicalization on social media and the internet involves preventing and prohibiting the spread of terrorist content and propaganda in the online space using digital mechanisms and tools. This includes: legislative and policy measures; blocking content and access to social media platforms; and filtering and removal of terrorist content from platforms. These mechanisms are intertwined, as the legislation around digital prevention can only be adapted and changed as new technological tools emerge in the space of prevention.

It should be noted that preventing the spread of terrorist content online involves leveraging technology and platforms that are usually owned by the private sector, so public-private partnerships and cooperation are critical in this particular strategy. One example of this sort of partnership is Tech Against Terrorism, an initiative developed in support of the United Nations (UN) Security Council Resolution 2354 (2017) to tackle terrorist narratives online. The project builds the capacity of smaller start-up companies and provides online tools for the private sector technology industry to prevent the spread of terrorist content on their platforms. The project involves multiple private sector companies, such as Facebook, and regularly works with the UN Security Council bodies.

**Legislative Measures: The Challenge of Creating Smart Regulation**

The first method for preventing the spread of terrorist content online is through the use of legislation and policies that set regulations for prosecuting individuals and organizations. Some legislation penalizes the content itself, making it illegal for individuals or companies to host content online. For example, although it does not directly address only terrorist content, the German Netzwerkdurchsetzungsgesetz (Network Enforcement Act, “NetzDG”) sets the penalties for spreading hate speech and fake news online for up to 5 million euros for individuals and 50 million euros for organizations. Under the definition of hate speech and fake news, the list of potential “unlawful” material include advocating actions against the democratic constitutional state, public order, personal honour, and sexual self-determination.

Other legislative measures focus more on the specifics of how the private sector should prevent terrorist content on their platforms. Since 2019, there has been increasing pressure on the private sector to step up its efforts. For example, with reference to a letter sent by the Chairman of the Homeland Security Subcommittee on Intelligence and Counterterrorism of the United States to members of the Global Internet Forum to Counter Terrorism (GIFCT) in
March 2019, Facebook, Twitter, Microsoft, and YouTube were requested to provide information on their annual budgets to curb extremism on their platforms. When information was not provided as requested, US Rep. Thomson and US Rep. Rose remarked in a press release;

“The fact that some of the largest corporations in the world are unable to tell us what they are specifically doing to stop terrorist and extremist content is not acceptable… broad platitudes and vague explanations of safety procedures aren’t enough. We need a full accounting of what is being done.”

Similarly, the European Parliament passed legislation called “Tackling the dissemination of terrorist content online” as a result of a 17 April 2019 resolution. The regulation aims to avoid the “misuse of hosting services for terrorist purposes and contributing to the public security in European societies.” The legislation focuses specifically on what can be done by “hosting services” - i.e. social media platforms - in content regulation and takedown. It should be noted that some of the more controversial parts of the plan, such as the requirement to take down terrorist content within one hour of posting, had been scaled back to give private sector companies more time to complete this task.

There are many challenges related to legislation and policy methods for preventing the spread of terrorist content online. Since policymakers tend not to be experts in communication technology, there is sometimes a misunderstanding of how internet and social media companies work, and which new technologies are available. There seems to be a general understanding from governments of how the mainstream social media platforms and tech giants operate (e.g. Facebook, Instagram, WhatsApp, Twitter, Microsoft, YouTube, and Google), but there is much less known about services offered by smaller companies such as Telegram, Signal, Ask.fm, Tumblr, Line, Kik, Qzone, Sina Weibo, Reddit, and many others. As new technologies such as AI and DWeb emerge, policymakers also struggle to keep up with the latest information and challenges associated with those technologies, and therefore are limited in their responses. Even less is known about how to moderate or regulate these platforms for preventing terrorist content online. In this regard, ensuring that governments and the private sector are working together in partnership is even more critical for smaller platforms that are less well-known.

As an example of this challenge, arguments against the EU’s Terrorist Content Regulation have expressed that the adoption of the legislation may lead technology and social media platforms to “adopt poorly understood tools” to address violent extremism and terrorism online, and that “lawmakers and the public have no meaningful information about how well the [tools] serve this goal, and at what cost to democratic values and individual human rights.” In other words, there is a lack of evidence that the proposed tools are actually effective at successfully preventing terrorist content from spreading, and the consequences of such aggressive takedown could lead to unintentional infringements of human rights (e.g. limiting freedom of speech), should those methods not be proven to be efficient or effective.

**Blocking Content and Access: Balancing Safety and Freedom of Expression**

One of the approaches to preventing terrorism online undertaken by a number of governments has been to block access to a terrorist group’s internet and social media channels. This has ranged from blocking individual websites and social media pages to blocking entire social media platforms. For example, in the aftermath of the 2019 Easter attacks on churches, hotels, and popular tourist sites in Sri Lanka, the government temporarily blocked all access to Facebook, Facebook Messenger, Instagram, WhatsApp, YouTube, and Viber. This temporarily restricted the communications channels in the face of the imminent threat of more attacks across the country, but it also restricted the ability of Sri Lankans, expats, and tourists
to communicate about their safety. In a similar way, Indonesia also blocked the popular social media application Telegram in 2017, after growing concerns of the influence of ISIS in the region and the use of Telegram in particular for spreading its messages on private Telegram channels.\(^{91}\)

While on one hand, blocking websites, social media pages and entire social media platforms slows down the spread of terrorist messages online, it also slows down normal communications channels for the rest of the population. That is, while temporarily blocking access to content may be effective for short-term crisis situations like the aftermath of the multi-pronged jihadist attacks in Sri Lanka, long-term blocking will end up forcing terrorist groups and the general population alike to seek alternative forms of communication. For example, in this way, if WhatsApp is blocked in one country, another application is likely to take its place that will have similar features, and the population - and the terrorists - will regain their ability to communicate. There have also been allegations that blocking access to social media content is an infringement of fundamental human rights, and that blocking content has been used to prevent the spread of ideas of political opposition groups. In this regard, governments may need to consider balancing their efforts to block websites with ensuring basic human rights under international law, and see to it that basic human rights are not violated by their actions.

Takedown and Filtering of Terrorist Content

A third way to prevent the spread of terrorist content online is through the takedown of individual posts or websites by technology companies themselves or by third parties. This can be done in several ways: requests from government entities to remove pieces of content; the self-regulation of technology companies to remove content; artificial intelligence such as “upload filters” and; through individual hackers and civil society-led content takedown.

In most of the known cases, government bodies ask private sector companies to remove content on their platforms if it is identified as terrorist content. This is done through careful cooperation between intelligence and law enforcement entities and those companies. For example, Europol’s Internet Referral Unit (EU IRU) is tasked to support EU authorities in flagging terrorist and violent extremist content online and sharing it with relevant partners. As of December 2017, the EU IRU assessed over 40,000 pieces of content across 80 platforms in ten languages, and 86% of the content flagged by this unit was successfully removed.\(^{92}\)

In addition to cooperating with governments, the main tech giants tend to have relatively elaborate policies to make it more difficult for their platforms to become havens for terrorist content. For example, Facebook’s counterterrorism policy states that there is no place for terrorism on Facebook, using an academic definition of terrorism that is predicated on behaviour - not ideology.\(^{94}\) Filtering and content takedown can be increased by the average social media user reporting on potential terrorist content, and Facebook’s policies have particular terms of use which requires users to abide by certain behaviours and rules - otherwise risking their profiles being suspended or blocked. Once a particular item or post is flagged by a user, there is a dedicated team of experts (content moderators) reviewing the content to decide if it should remain online or offline. Twitter’s policy around terrorism is similar in that its users “may not threaten or promote terrorism or violent extremism.”\(^{95}\) Twitter users can report Tweets that violate this policy, indicating that it is “abusive or harmful” and “threatening violence or physical harm.”\(^{96}\) YouTube has also developed a “Trusted Flagger” program which consists of individuals, government agencies, and NGOs working in various locations across the world that actively monitor content on YouTube, and flag content that violates their Community Guidelines.\(^{97}\) The purpose of this program is to ensure that there are relevant local experts that understand the contextual and linguistic nuances of content being uploaded online.
The content flagged by the “Trusted Flagger” program receives higher priority for review by content moderators.

Another way for social media platforms to remove terrorist content from their platforms is through the use of AI. For example, image matching systems categorize previously removed terrorist content, and block the upload of new images or videos that are the same. The GIFCT has developed a “Hash Database”: a shared list of the “hashes” or unique digital fingerprints of terrorist imagery and recruitment videos. Members of the GIFCT are able to share new content with each other so that it can be removed before it spreads online. However, it should be noted that there are certain limitations to this database - notably that the “hashes” have to be exact matches to the original file data. In this way, images or videos that are manipulated slightly by users will not match the “hash” and therefore would not be recognized by the AI systems. In the meantime, social media companies are working with more sophisticated AI tools internally to become better and smarter at recognizing terrorist content automatically on their platforms.

In an April 2019 resolution taken by the EU, it was suggested that it become mandatory for companies to use “upload filters” - technological mechanisms that prevent content from being uploaded to social media sites if suspected of being terrorist content. The pressure to implement “upload filters” was exacerbated after the Christchurch attack in March 2019 - where the perpetrator live-streamed the attack on Facebook. Facebook subsequently reported that it removed 1.5 million videos circulated afterwards. However, it should be noted that the effectiveness of “upload filters” and AI mechanisms is still unknown, and more research is needed in this field to ensure the technology and content detection are evolving as the terrorist threat evolves. As such, at the same time that social media companies continue to improve their AI systems, regulatory bodies should also factor in new technologies - and their limitations - in automatic content detection to their new policies.

Individuals also have the ability to directly combat terrorist propaganda online. As an example, a group of hackers linked to the “Anonymous Collective” also “declared war” on ISIS’ online accounts and propaganda through #OpISIS, a hacking campaign that aimed to report, interfere and disrupt suspected ISIS accounts. The campaign initially exposed 70 ISIS-linked websites and 26,000 Twitter accounts being used for recruitment, communications, and intelligence-gathering, which were later investigated and taken down by authorities.

There are several challenges with content takedown on social media platforms. First of all, content takedown requires a certain level of knowledge of the material (e.g. terrorist content) by those moderators charged with removing it. In some circumstances, human content moderators are faced with difficulties discriminating between legal and illegal content, and often face a “grey area” making it hard to decide whether something should or should not be considered in violation of company policies. For example, would a historical photo of Germany with Nazi flag in the background be considered neo-Nazi propaganda? The determination of how this might be a violation of company policy may depend on the context, comments and placement of the photo on the platform by the user. Appropriate staff training and expertise is needed to ensure appropriate content takedown - which of course requires resources. While these resources may be more readily available for larger companies, smaller platforms struggle to keep up with the knowledge and resources required for preventing terrorist content on their platforms.

Moreover, even the larger companies struggle to employ experts that have nuanced language and cultural expertise. For example, Facebook came under fire by the media over its inability to take down hate speech on Rohingya in Myanmar in April 2018. Reuters was able to find over 1,000 examples of posts, comments and images attacking Rohingya communities on Facebook, which resulted in Facebook reacting by ramping up operations and more closely monitoring content in Myanmar. Facebook was originally not equipped to handle the hate speech online due to a lack of experts with Burmese language and cultural
skills, the use of slang and obscure language used to identify target groups, and the sheer volume of hate speech against the Rohingya community, something not anticipated by Facebook at the time.

In the same vein, as removing and filtering terrorist content slows down the flow of terrorist propaganda, it does not stop it entirely. One critic explained the challenge using the “Whack-A-Mole” metaphor - alluding to the “amusement park classic where one takes a mallet to a seemingly unending set of furry rodents that pop up at random from holes in a big board.” When content is taken down from one website, a replacement (or several) is made on a different channel. The online environment is constantly changing, and those charged with content takedown and filtering are met with an unending and exponentially growing supply of the same material appearing across different platforms.

**Countering the Narratives of Violent Extremism and Terrorism Online**

A second strategy for preventing radicalization on social media and the internet is related to countering (directly or indirectly) the narratives of violent extremism and terrorism in the online/digital space. The terminology of “counter-narratives” has been hotly debated in the CVE community, and while a robust debate of the definition of a counter-narrative is outside the scope of this chapter, it is important to take a commonly accepted definition of a “counter-narrative” as an attempt “to challenge extremist and violent extremist messages, whether directly or indirectly through a range of online and offline means.”

There are several points related to this strategy worth mentioning. First of all, the strategy of countering narratives in the online space should always take into consideration the target audience through the local context. If a counter-narrative does not address the grievances or needs of those joining terrorist groups, or counter the attractions of terrorist propaganda, then the counter-narrative surely will not be effective. This can be accomplished partially through empowering communities, both online and offline, with the appropriate knowledge, skills and tools to contest and counter the messages of violent extremism and terrorism in their networks. In this sense, some organizations have provided capacity-building to “local voices” as part of their broader communications campaign against terrorism. An example of this approach is the Kenya-based YADEN’s #insolidarity campaign. The initiative provides capacity-building, tools, and platforms for youth to develop their own messages and share their stories about how terrorism has influenced their lives.

Second, it is recommended that the design and structure of a counter-narrative focus on the development of a counter-narrative that is tailored to a specific target audience. Hedayah has developed a “How-To Guide” as well as several capacity-building modules that provide guidance for organizations looking to enhance their counter-narratives and campaigns. The nine steps outlined in Hedayah’s framework take a marketing perspective that is needs-based, whereby the context and target audience are carefully defined in the beginning of the process. This process is consistent with the integrated marketing communications (IMC) approach whereby significant research on the target audience is conducted at the outset, and strategic messages simultaneously target decision-makers and peripheral observers to achieve the maximum impact. As one youth-worker from Kenya noted, terrorists use this same strategy in their communications techniques: “propaganda is seen as ‘rebel cool’ because it shows defiance and rebellion against governments.” On the other hand, their organization’s peaceful protests were sometimes viewed by the community with scepticism, noting that their organization received complaints when police did not show up or aggressively confront protesters “because it is ‘cool’ to be seen as rebellious.” In this example, the actions taken by the youth organization were rejected by their target audience because it was not adapted to their perceptions of being “cool.”
Once the target audience is identified, one of the most critical steps is to determine which messenger would be most effective at influencing that target audience. In this case, the counter-narrative needs to critically integrate a messenger that the target audience is most likely to listen to. For example, in Pakistan, the pop star Haroon created a cartoon series called *Burka Avenger*, based on a teacher at a girls’ school fighting evil with books, pens, and martial arts. As a messenger, Haroon’s celebrity status drew in an audience for *Burka Avenger* to deliver messages of peace, tolerance, acceptance, cooperation, gender-equality, and other critical values. Although the message was not necessarily designed to counter terrorism, the messenger for these positive messages was effective at reaching a broader and more relevant audience.

Finally, the content of a counter-narrative needs to both be attractive, but also provide the right information that prevents individuals from being allured by the terrorist group. This can be done in several ways: deconstructing terrorists’ arguments (pointing out where they got the facts wrong); undermining the credibility of the group; and providing alternative narratives that emphasize non-violent actions. It is also crucial that counter-narratives are complemented by positive actions; mere words and pictures are not enough to persuade most dissatisfied people if unaccompanied by credible and matching deeds.

**Deconstructing Terrorist Arguments**

The first way of preventing terrorism online through counter-narratives is by directly engaging with and deconstructing the arguments of terrorist groups. Despite the direct engagement with terrorists or potential terrorists, the target audience for this type of strategy is actually not the individuals or group themselves - but the broader “theatre” of those that might be watching, listening, and following publicly-available forums. A specific example of this sort of deconstructive “theatre” can be seen through the public debate on Twitter between journalists, scholars, and religious leaders and the American Al-Shabaab terrorist Omar Hammami. Some narratives aimed at Hammami attempted to persuade him to turn himself in, and exploited the schism between Hammami and Al-Shabaab’s leadership as an entry point. For example, after an attempt on Hammami’s life by Al-Shabaab, J.M. Berger tweeted, “Looks like you were within a quarter inch of dying… Perhaps it’s time to come in now.” Others deconstructed his ideological and religious claims, using the Qur’an and Sunnah to contradict the justifications Hammami was making about jihad and his struggle against the West. While Berger was also hoping to personally persuade Hammami to surrender, it also had the effect of delivering a message to those followers closely watching Hammami’s accounts.

**De-legitimizing Terrorist Groups and Actions**

A second counter-narrative method is to de-legitimize the message of terrorist groups by exploiting inaccurate information disseminated by terrorist groups, or leveraging humour and sarcasm to discredit a particular message or the organization as a whole. It is hypothesized that leveraging the voices of former terrorists (“formers” or “defectors”) can assist in discrediting the group, and indeed some counter-narratives have exploited this idea. Formers can draw attention to the hypocrisies of a group, such as highlighting corruption or injustice, or speaking to a reality that is inconsistent with what is promised by propaganda videos and recruiters. For example, Abu Abdallah, a former ISIS soldier, explained the oppression, punishments, and killings that took place under the rule of ISIS in Syria in an Arabic-language video “Inside ad-Dawlah.” Areeb Majeed, a suspected ISIS member from India, explained how he had been asked to conduct “menial tasks like cleaning toilets or providing water to those on the battlefield, instead of being pushed into the warzone” partially due to racial discrimination because “Indians were considered physically weak.”
Humour and sarcasm can also be used to discredit terrorist groups. One example is the case of Japan “winning the internet” through a technique Huey calls “political jamming,” or “a subversive, satirical activity that draws on humour to reinforce ideological messages.” After the 20 January 2015 release of an ISIS YouTube video of two Japanese hostages, Kenji Goto Jogo and Haruna Yukawa, the Japanese public responded with screenshots of the video, photoshopped to ridicule ISIS. The hashtags #ISISCrappyCollageGrandPrix and #ISISPhotoshopGrandPrix encouraged more memes and photoshopped images to circulate. The message from Japan to ISIS was clear: the Japanese were not intimidated by ISIS.

Positive Messages and Alternatives to Terrorism

Finally, instead of countering - or reacting to - the messages of terrorist groups, preventing terrorism online can focus on promoting positive and alternative messages to terrorism. These messages can address both structural or personal grievances such as building positive identities and enhancing social cohesion. There are several examples of alternative narratives worth mentioning here. In the Indonesian context, the Nahdlatul Ulama (NU), one of the largest Muslim organizations in the world, has been conducting a campaign focused on highlighting Islam Nusantara, or Indonesian Islam, the tenants of which are outlined in a 90-minute film, “The Divine Grace of Islam Nusantara.” The principles of Islam Nusantara emphasize the religious and cultural identity components of Islam in Indonesia that are uniquely Southeast Asian, and run contrary, in some cases, to more Salafist interpretations of Islam that are perceived by some to be “foreign.” In March 2019, the NU announced that they recommend eliminating the use of the Arabic word kafir (infidels) to describe non-Muslims, and instead advocated for the use of the word muwathinun to emphasize that both Muslims and non-Muslims were equal in terms of citizenship in Indonesia.

One important component of alternative messaging is to provide a non-violent action that still addresses grievances that communities might have which can be underlying drivers of radicalization. For example, in South Sudan, the Anataban (meaning “I am tired”) campaign supports the “tired” people of South Sudan through music and art that promotes peaceful and non-violent movements. A video published in 2017, “Soutna,” meaning “Our Voice,” states “we need peace desperately in order to achieve a bloodshed free 2017,” encouraging users to use #Bloodshedfree2017 on their social media posts. The video shows young South Sudanese peacefully demonstrating in their communities and participating in actions such as voting and stating “we raise our voices to peace.” The Anataban movement recognizes that violence and corruption are normalized in South Sudan and citizens are encouraged to take proactive steps towards peace while not tolerating violence in their communities.

Developing counter-narratives does not come without criticisms or challenges. First, there is always the question around how these efforts can be measured and evaluated. There are very few studies that look at the impact and effectiveness of counter-narratives, although this body of literature is growing with efforts to find communications solutions that work in the space of terrorism prevention. Some studies have attempted to evaluate the effects of counter-narrative campaigns. For example, an initiative by students at Simon Fraser University in Vancouver, Canada, created the “Voices Against Extremism” project which included several components. The “Stories of Resilience” campaign featured students and average Canadians explaining “how extremism has affected their lives as well as their thoughts and opinions on community and Canadian identity.” It also included a YouTube video titled “An Evolution of Violent Extremism &Terrorism” to provide more information to students on the effects of violent extremism, and featured an art gallery event called “Art is H.E.R.E: Reshaping Identities.” The project reached over 160,000 individuals on their online campaigns, and an additional 100 individuals (students) through their offline engagements. However, the
evaluation of the campaign included largely superficial measurements; there is no evidence of impact on cognitive and behavioural changes.

Another study by McDowell-Smith, Speckhard and Yayla (2017) examined the effects of counter-narrative videos on the perceptions of college students in the US. The study showed several video campaigns using defectors from ISIS to a group of college students and asked them to provide information on their perspectives regarding the effectiveness of the campaign. One critical limitation to this study was, of course, that the average US college student is not radicalized, and therefore the effectiveness of the campaigns can only be considered in terms of a wider “youth” population, but not with respect to the potential target population of youth that may be interested in joining ISIS.

Perhaps one of the best in-depth studies specifically on counter-narratives was conducted by the Institute for Strategic Dialogue on three counter-narrative campaigns: “Exit USA,” “Average Mohammad,” and “Harakat ut Taleem.” This study seems to be unique in that it starts to look at measures of engagement and impact, rather than simply measures of the scope or reach of the campaigns. Using analytical tools such as assessing the sentiment of the comments or anecdotes of sustained engagement (both constructive and antagonistic), this study started to examine the potential impact of the campaigns on changing attitudes of the target audience. For example, the “Exit USA” campaign had the effect of soliciting a sustained engagement with a former white supremacist who was thinking of returning to the group, and managed to persuade him to participate in Exit USA’s activities, thereby deterring him from re-engaging from the group.

Second, there are potential considerations for “blowback” if certain parts of the message or the messenger are not right, and there have been examples where campaigns against violent extremism have actually made the problem worse. Campaigns countering the message of terrorist groups may provide a platform for terrorists to make their arguments in a more public way - drawing attention to their arguments rather than detracting from them. A frequently-cited example of the “blowback” effect of a communications campaign is that the media coverage on Iraq and Afghanistan, specifically the coverage of detention facilities in Guantanamo Bay and Abu Ghraib, reduced the support on the ground in these countries for the American actions there.

The third challenge relates to some communications strategies that have attempted to flood the Internet with messages directly countering terrorists’ messages in the hopes that this would overwhelm communications channels with the “right” messages. The US Department of State also took on this strategy through the Center for Strategic Counter-Terrorism Communications (CSCC), now relabelled Global Engagement Center, whereby their digital outreach team (DOT) “crash[ed] various online forums to troll ISIS sympathizers and regularly jumps onto pro-ISIS Twitter hashtags.” By “hijacking” the hashtags, CSCC’s DOT intended to make available a larger quantity of counter-messages than the violent extremist content. However, there is little evidence to suggest that this approach has been effective at reducing the appeal of terrorism or preventing radicalization online. This is because the trajectory from the development and distribution of a communications product to the consumption of its message to the potential impact on an individuals’ behaviour is a complex process. Research suggests that most participants in foreign fighting and/or terrorist activities are not primarily recruited online, but rather by “real-world” connections to social networks. As Archetti outlines, consumers of information engage in an active selection of the materials on which to focus, meaning consumers only “buy” into the information that catches their attention or appeals to them in some way. In this sense, the mere availability of a message, or the number of times it appears to have been viewed, does not directly translate into interest, or impact on cognitive processes, let alone impact on behaviour. Obviously, availability alone is not correlated with behavioural change; all individuals that view a video by ISIS online do not necessarily become radicalized. Otherwise, there would be a very strange pool of “radicalized”
counterterrorism experts and researchers that regularly view terrorist content in the hope to understand the content and messaging techniques used by various terrorist organizations. At the same time, and what is easily illustrated by the spread of terrorist messages, is that few individuals can be responsible for an idea that goes “viral” and reaches a large audience. According to Malcom Gladwell’s Law of the Few, 20% of participants are responsible for 80% of the work as long as that 20% includes the right mix of actors: connectors, or those that bring the network together; mavens, or those “experts” that provide new information to the group; and salesmen, or those that bring charisma and powerful negotiating skills to the participants. Saifudeen argues that groups like ISIS and Al-Qaeda have adopted a communications model that applies this theory. ISIS “fanboys” are the connectors that spread the message easily to their networks, fighters are the mavens that offer information and experience from the battlefield, and leaders like Anwar al-Awlaki are the salesmen that give credibility and charisma to the ideas.

Last, there seems to be a lack of emotional appeal for many of the counter-narratives that are devised and constructed online, especially those that are more direct and targeted towards terrorist content. For example, the Religious Rehabilitation Group (RRG) operating out of Singapore provides a point-by-point deconstruction of the ideologies leveraged by groups such as Al-Qaeda and ISIS in an attempt to discredit them. However, as Archetti puts it, “Narratives… are much more than rhetorical devices… they have deep roots: they are socially constructed.” Ferguson also argues that, “questions around why certain [violent extremist] VE narratives can be so powerful are rarely addressed in detail in contemporary grey CVE literature… VE narratives are successful… because they tap into, and seemingly confirm, existing beliefs of anxieties.” The narratives that terrorist groups offer are highly emotional, and therefore the counter-narratives need to reflect this same principle.

Building Digital Resilience and Media Literacy

In today’s digital age, there is a massive challenge related to “fake news,” “misinformation,” and “disinformation,” which are tactics employed by political actors and terrorist groups alike. A third and final strategy for the prevention of terrorism online is through building digital resilience and media literacy skills. This is premised on two assumptions. Firstly, that by building digital resilience and media literacy, the average citizen is able to peacefully overcome grievances that might lead to radicalization that are based incorrectly on misinformation or disinformation. Secondly, that a citizen that is able to evaluate both the content of the information provided and the credibility of the source more effectively, would less likely be persuaded by terrorist propaganda.

The terms “fake news,” “misinformation,” and “disinformation” are sometimes used interchangeably, so it is first of all important to define these terms for the purposes of preventing terrorism. “Fake news” can be defined as “fabricated information that mimics news media content in form, but not in organizational process or intent,” whereas “misinformation” is “false or misleading information, and “disinformation” is “false information that is purposely spread to deceive people.” All of these types of content are leveraged by many different kinds of actors (including politicians and terrorist groups) - and are not always intended to do harm. However, these tools are also employed by terrorist organizations, and can have the effect of exacerbating structural or societal grievances or other push factors that may lead to radicalization or recruitment. Moreover, these tactics may emphasize underlying black-and-white thinking or encourage polarizing worldviews that lead to divisions in society. These tactics can also play upon pull factors that may make a terrorist group or ideology seem more attractive. Combined with divisive rhetoric used in hate speech and by terrorist groups that exacerbate “us” versus “them” thinking, tactics employing “fake news,” “misinformation,” and “disinformation” can be dangerous.
It is important, therefore, that skills and mechanisms for building digital and media literacy are enhanced as part of a comprehensive way of preventing terrorism online and in social media. This means that potentially vulnerable youth should be equipped with the appropriate skills to navigate the challenging communications environment they experience every day, including a large social media presence online. This environment is often filled with conflicting messages - and determining which of those messages are credible and which are false is a complex skill to be cultivated. This approach has been adopted in UNESCO’s preventing violent extremism (PVE) efforts, noting the importance of responsible behaviour online and offline as part of an individual’s responsibility as a “digital citizen.”

Even ISIS has caught on to the importance of digital and media literacy, but has distorted this concept to serve its own aims. For example, in an infographic titled “Rumors,” ISIS warns against the danger of rumours that “distort a person or a group of Muslims,” or “demoralize the Muslims in times of hardship,” or “dividing the Muslims and making problems between them,” among others. The infographic was accompanied with advice on how to fight rumours, and how these can be damaging to Muslims.

The formal education sector also plays a significant role in ensuring students are able to differentiate between various kinds of tactics that are used by terrorist groups to spread their messages. To aid the education sector, there are a number of resources available to teachers to better enhance their abilities to teach students about digital resilience. For example, UNESCO has a number of tools, including a framework and assessment tools, to monitor the progress of digital literacy skills worldwide, in support of Sustainable Development Goal #4 on Quality Education. The framework provides guidelines on a number of different digital competencies that include:

- Information and data literacy (e.g. browsing, searching, and evaluating data online);
- Communication and collaboration (e.g. interacting, sharing, and collaborating using digital technologies);
- Digital content creation (e.g. developing digital content, copyrights, and licensing);
- Safety (e.g. protecting devices, personal data, and well-being); and
- Problem solving (e.g. identifying needs and digital/technical responses).

It goes without saying that the digital literacy framework is broader than supporting terrorism prevention online, and is intended to be integrated into school systems globally.

Social media and technology companies have also dedicated quite a few resources to educating the public on digital and media literacy skills. For example, Google for Education also has a number of digital tools for teachers that provide educators with ways to bring hands-on learning to digital and media literacy. They have a suite of lesson plans, activities, and video tutorials dedicated to assisting teachers in cultivating digital skills in their students. Facebook also has developed a Digital Literacy Library comprised of lesson plans designed to help youth develop digital skills, both inside and outside the classroom.

While digital and media literacy of course have other possible effects in addition to preventing terrorism, digital resilience for the purpose of terrorism prevention should focus on verifying the credibility of the sources and methods of the content under question. The Tony Blair Institute for Global Change suggest the “RAVEN” method for determining the credibility of Internet sites in relation to identifying terrorist propaganda:

- Reputation: The student examines the credibility of the website or author.
- Ability to see: The student questions if the person writing is in a position to be well-informed about the issue.
- Vested interest: The student questions if the author stands to gain anything by having a certain point of view.
• Expertise: The student questions if the author is qualified to know what s/he is talking about through training or background.

• Neutrality: The student questions if the content is neutral, and if not, why the author might be taking a particular point of view.

While there are other methods in existence, the critical point of digital literacy for students in this case is to ensure that students really understand the credibility of the source before it is trusted as fact or shared with others.

Another way that sources can be checked is through fact-checking websites. For example, Snopes.com is a tool that can check the content of a webpage to verify against other known sources to determine whether the content is likely factually-based. In some cases, Snopes.com has been able to identify hate speech online. For example, in May 2019, Snopes reported on how anti-Islamic hate speech, revealed by their fact-checking technology, was being spread on Facebook through a particular network. As a result of the investigation, the network and forum for this hate speech was reportedly disabled. The government of Indonesia has also undertaken a similar initiative through its TRUST Positif website. Here, internet surfers can insert a URL and verify whether or not a given source is a trusted domain name. Smaller companies dedicated to fact-checking for social good are beginning to evolve on social media platforms, and these tools can be leveraged to avoid the spread of “fake news,” “misinformation” and “disinformation,” some of which is affiliated with terrorist groups.

Conclusion

This chapter highlighted that terrorist organizations are continuously adapting to the evolving technologies and are particularly adept at using social media and the internet for radicalization and recruitment purposes. However, this chapter also notes a number of potential approaches which could contribute towards terrorism prevention.

Firstly, a public-private cooperative and inclusive approach was found to be most important, contributing to the enhancement of all prevention efforts. As noted, there is a distinct lack of understanding within the public sector on how exactly most of these platforms operate and the types of responses these can feasibly take. This was found to be especially the case for smaller, lesser-known online platforms. Hence, it is important to coordinate and consult with all relevant providers when developing legislation and policies, as well as for practical responses. On this note, realistic legislation that sets regulations for prosecuting individuals and organizations, penalizes the content, and makes it illegal to host such content on a platform is also seen to be a valuable response; provided that private sector representatives are engaged during development, to ensure achievability.

Another approach is the blocking of access to content shared by terrorist groups. However, it should be noted that the blocking of entire platforms has unintentional effects on the general population and there is a significant risk of infringing upon universal human rights. Furthermore, online platforms tend to be resilient; when one platform is blocked, another will often surface in its place. Therefore, a potentially more effective approach, although often requiring more man-power and time, is takedowns of terrorist content. While this is primarily implemented as per the private organizations’ own policies, it would also benefit from strong public-private cooperation and collaboration, whereby government agencies can inform platform providers of content to be removed. Additionally, this can be further enhanced by awareness raising and the encouragement of a whole-of-society approach, where every user understands the importance of her or his role in flagging and referring any online content that is in breach of such policies. Those who are responsible for the decision on whether a takedown is required also need further training, particularly in relation to localizing their knowledge and understanding. Having a clear comprehension of the local language and culture will greatly
enhance their decision-making skills on whether specific content should be removed, thereby increasing the effectiveness of the response overall.

On the other side of the coin is “upload filters,” which also could be seen to be a proactive and efficient means for prevention. However, the effectiveness of such an approach has yet to be proven and the technologies for doing so are not yet mature enough to definitively work independently of human review and action.

While these approaches may help to contain the spread of online terrorist propaganda, they will not necessarily stop the flow entirely. Therefore, there is also a need for additional approaches which can address the propaganda that leaks through. One such approach is that of counter-narratives. While the effectiveness of this approach is still disputed, developing a comprehensive counter narrative strategy which delegitimizes and deconstructs the terrorists’ narrative and produces positive and alternative narratives, may assist with addressing the structural and personal grievances which leave individuals and groups vulnerable to radicalization. In this regard, there is a need to enhance the skills - and amplify the dissemination - of those who are appropriately positioned to produce counter narratives, such as former violent extremists and creative young activists, in a manner that is locally tailored, targeted and relevant.

However, there will still be cases where the terrorists’ propaganda reaches the target audience, but the counter narratives do not. Therefore, there is also a need to build the resilience of individuals, especially in the form of digital resilience and media literacy. In this regard, global education sectors have a significant role to play and should adapt their curriculum to include approaches that would provide youth with the understanding and skills to question the credibility of sources more effectively, thereby decreasing the likelihood of being persuaded by terrorist propaganda. It is noted that some governments and private organizations have started to engage in this field. However, at the current stage, the further enhancement of these efforts could be a useful step for governments to take.

Finally, it should also be noted that while these approaches are preventative, they are also reactive in development, based upon previous experiences and the ongoing methods used by terrorist groups. It is of the utmost importance for governments and online platform providers to be forward-looking: assessing how the platforms may be exploited in the future and what possible forthcoming platforms may play a role in radicalization and recruitment. The effective identification of possible future threats will allow for more proactive prevention strategies and ensure positive outcomes.

Sara Zeiger is the Program Manager for the Department of Research and Analysis at Hedayah, the International Center of Excellence for Countering Violent Extremism in Abu Dhabi. Sara Zeiger supports the Director in managing the Department’s resources and programs, including the Counter-narrative Library, Hedayah’s non-resident Fellowship Program and Hedayah’s annual International CVE Research Conference. Sara was also the lead content developer for Hedayah’s App, MASAR, that provides practical guidance on MM&E for CVE. She has also been a co-Director for a NATO Science for Peace and Security (SPS) grant on enhancing the role of women in international CVE efforts. In addition to her duties in the Department of Research and Analysis, she was also Hedayah’s liaison with the Global Counterterrorism Forum (GCTF) to support the development and drafting of their framework document, the “Abu Dhabi Memorandum on Good Practices for Education and CVE” and the follow-up “Action Plan”. Sara Zeiger is currently a Non-Resident Fellow in International Relations and Counter-Terrorism for TRENDS Research & Advisory. Prior to joining Hedayah, Sara worked as a Research Assistant at the Center for Middle Eastern Studies at Harvard University. She also served as a Head Teaching Fellow for the Harvard Extension School where she taught courses on anthropology in the Gulf, politics in the Middle East, and
Islam in the West. Sara Zeiger holds a Master’s in International Relations and Religion (concentrations: Security Studies and Islam) from Boston University, and graduated as valedictorian with a B.A. in Psychology and Religion from Ohio Northern University.

Joseph Gyte is the Senior Program Associate within the Capacity Building Department at Hedayah, the International Center of Excellence for Countering Violent Extremism in Abu Dhabi. Joseph Gyte supports the curriculum development, implementation and evaluation of capacity building programs, and leads a program for psychologists and social workers to support families affected by violent extremism. Prior to joining Hedayah, Joseph Gyte worked as a Terrorism Prevention Program Consultant at the United Nations Office on Drugs and Crime (UNODC), Regional Office for Southeast Asia and the Pacific. In this position, he acted as focal point for the planning and implementation of capacity building activities related to Counter Terrorism in Indonesia, Myanmar and the Philippines. He also contributed technical inputs towards the development of a National Action Plan to Prevent Violent Extremism in a Southeast Asian country, and produced multiple training manuals, handbooks, publications and Op-Eds, on behalf of UNODC. Joseph Gyte has also worked in the Office of the EU Counter-Terrorism Coordinator in Brussels, where he was directly involved in the EU’s development of policy responses to the evolving phenomena of foreign terrorist fighters and violent extremism. Joseph Gyte’s educational background includes a Master’s degree in Terrorism Studies from St. Andrews University and a Bachelor’s degree in Psychology from Cardiff University.
Endnotes


3 Perliger, Arie, ‘Terrorist Networks’ Productivity and Durability: A Comparative Multi-Level Analysis,’ Perspectives on Terrorism, 8(4), 2014, pp. 36-52.


12 For the purpose of this chapter, “Brand Management” is used to refer to the techniques employed by terrorist groups to maintain and increase the perceived value, importance and reputation of the group.


18 Weis, Caleb, ‘Philippines-based Jihadist Groups Pledge Allegiance to the Islamic State,’ FDD’s Long War Journal, 2016. Available at:


20 Atwan 2015.


22 Macnair and Frank 2017.


25 Ibid.


39 These responses, which include monitoring and takedown, will be discussed in greater depth in the following section.
46 Atwan 2015.
47 Lombardi 2015.
49 Nissen 2014.
51 Nissen 2014.
54 Associated Press, ‘Christchurch Mosque Shootings: Gunman Live Streamed 17 Minutes of Shooting Terror,’ New Zealand Herald, 15 March 2019. Available at:

55 Facebook Newsroom, 17 March 2019. Available at: https://twitter.com/fbnewsroom/status/1107117981358682112.
56 Waters and Postings 2018.
57 Lombardi 2015.
58 Associated Press, ‘Swedish Isis fundraiser statuses were on Facebook for two years before deletion,’ The Local, 25 March 2018. Available at: https://www.thelocal.se/20180325/swedish-isis-fundraiser-statuses-were-on-open-facebook-page-for-two-years-before-deletion.
59 Waters and Postings 2018.
60 Atwan 2015.
64 Atwan 2015.
65 Dunlap, Justine A., ‘Intimate Terrorism and Technology; There’s an App for That!’ University of Massachusetts School of Law, 2014. Available at: https://scholarship.law.umassd.edu/cgi/viewcontent.cgi?article=1028&context=fac_pubs.
66 Stalinsky Sosnow 2015.
69 Institute for Policy Analysis of Conflict (IPAC) 2015.
70 Ibid.
71 Atwan 2015.
72 Weimann 2015.
73 Ahmed, Mubaraz and Fred Lloyd-George, ‘A War of Keywords: How Extremists are Exploiting the Internet and what to do about it,’ The Tony Blair Institute for Global Change, 2017. Available at: https://institute.global/sites/default/files/inline-files/IGC_War%20of%20Keywords_23.08.17_0.pdf.
74 Stalinsky and Sosnow 2016.
76 GPT-2 is an open-source unsupervised language model developed by Open AI that generates coherent paragraphs of text, performs reading comprehension, machine translation, question answering, and summarization without task-specific training.


82 Tech Against Terrorism, ‘Project Background (Online),’ Tech Against Terrorism, 2017. Available at: https://www.techagainstterrorism.org/project-background/.


87 Ibid, p. 3.


Ibid.


Facebook Newsroom, 17 March 2019. Available at: https://twitter.com/fbnewsroom/status/1107117981358682112.


Ibid.

Peritz, Aki, ‘What Whac-A Mole Can Teach Us About How to Fight Terrorism,’ Foreign Policy, 12 August 2015. Available at: https://foreignpolicy.com/2015/08/12/what-whac-a-mole-can-teach-us-about-how-to-fight-terrorism/.


Zeiger 2018.

Ibid.

Ibid.


International Center for the Study of Violent Extremism (ICSVE), ‘Inside ad-Dawlah,’ ICSVE, 2017. Available at: https://m.youtube.com/watch?time_continue=17&v=fKw6j-Z9u64.


Huey, Laura, ‘This is not your Mother’s Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming,’ Journal of Terrorism Research, 6, 2015.

Ibid.

International Institute of Qur’anic Studies, ‘The Divine Grace of Islam Nusantara – Trailer,’ International Institute of Qur’anic Studies, 2015; Available at: https://m.youtube.com/watch?time_continue=11&v=aLEi5ED_-Xw.


Anataban South Sudan, ‘Soutna by #Anataban South Sudan Music 2017,’ Anataban South Sudan, 2017. Available at: https://m.youtube.com/watch?v=196d9E0XI_4.


Macnair and Frank 2017.

McDowell-Smith, Speckhard and Yayla 2017.


Ibid.


Schmid 2014.

Cottee and Hayward 2011.


132 Archetti 2015.

133 Ferguson 2016.


140 Ahmed and George 2017.


142 Ibid.

143 Ministry of Communication and Information Technology, Government of Indonesia 2010.
Ahmed, Mubaraz and Fred Lloyd-George, ‘A War of Keywords: How Extremists are Exploiting the Internet and what to do about it,’ The Tony Blair Institute for Global Change, 2017. Available at: https://institute.global/sites/default/files/inline-files/IGC_War%20of%20Keywords_23.08.17_0.pdf.


Anataban South Sudan, ‘Soutna by #Anataban South Sudan Music 2017,’ Anataban South Sudan, 2017. Available at: https://m.youtube.com/watch?v=196d9E0Xl_4.


Associated Press, ‘Swedish Isis fundraiser statuses were on Facebook for two years before deletion,’ The Local, 25 March 2018. Available at: https://www.thelocal.se/20180325/swedish-isis-fundraiser-statuses-were-on-open-facebook-page-for-two-years-before-deletion.


Dunlap, Justine A., ‘Intimate Terrorism and Technology; There’s an App for That!’ University of Massachusetts School of Law, 2014. Available at: https://scholarship.law.umassd.edu/cgi/viewcontent.cgi?article=1028&context=fac_pubs.


Facebook, ‘Digital Literacy Library,’ Facebook, 2018. Available at:

Facebook Newsroom, 17 March 2019. Available at: https://twitter.com/fbnewsroom/status/1107117981358682112.


Huey, Laura, ‘This is not your Mother’s Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming,’ Journal of Terrorism Research, 6, 2015.


International Center for the Study of Violent Extremism (ICSVE), ‘Inside ad-Dawlah,’ ICSVE, 2017. Available at: https://m.youtube.com/watch?time_continue=17&v=fKw6j-Z9u64.


Ministry of Communication and Information Technology, Government of Indonesia, Trust Positif, 2010; Available at: https://trustpositif.kominfo.go.id/


Peritz, Aki, ‘What Whac-A Mole Can Teach Us About How to Fight Terrorism,’ Foreign Policy, 12 August 2015. Available at: https://foreignpolicy.com/2015/08/12/what-whac-a-mole-can-teach-us-about-how-to-fight-terrorism/.


Tech Against Terrorism, ‘Project Background (Online),’ Tech Against Terrorism, 2017. Available at: https://www.techagainstterrorism.org/project-background/.


Chapter 13

Prevention of Recruitment to Terrorism

Ahmet S. Yayla

The long-term survival of terrorist organizations relies on their ability to attract new members and maintain an ongoing terrorist recruitment cycle. The numbers of terrorist organization members may decrease due to counterterrorism operations or defections, forcing the leaders of those groups to seek new members. Preventing terrorist recruitment is one of the most effective and least lethal methods of countering terrorism, and yet it is often overlooked by those combating terrorism. Western governments did not stop Al-Qaeda from recouping its losses, even after it suffered devastating losses in the months following the 9/11 attacks. The fact is that Al-Qaeda had only around 400 armed members at the time of 9/11, as opposed to thousands of affiliated members in 2019. Although the recruitment strategies of different organizations may vary, they follow a similar historical pattern. All recruiters must first identify qualified candidates, then establish secure connections, build rapport, indoctrinate them, and slowly pull them into an organization. ISIS proved that this process could be fast-forwarded through online propaganda and social media. Preventing recruitment in the first place can be the most fruitful, and maybe also least expensive, method used to counter terrorism. Successfully short-circuiting the recruitment cycle may save thousands of lives of prospective recruits and many more lives by thwarting future attacks. This chapter aims to present a holistic and comprehensive road map for interrupting and preventing terrorist recruitment by identifying relevant societal factors and triggers that recruiters use to find and control their subjects.

Keywords: Terrorist recruitment, prevention, terrorism, intervention, countering terrorism, family involvement.
Preventing terrorist recruitment is one of the least lethal and most practical, inexpensive, and humane ways of countering terrorism, both in the short- and long-term. However, historically, preventing recruitment to terrorism has often been ignored or considered a less appealing method of countering terrorism. Often, counterterrorism authorities rightly focus on being able to provide immediate security and prevent terrorist attacks by carrying out counterterrorism operations or targeting operators who have already been recruited into the ranks of terrorist organizations. While these operations may provide much-needed short-term security and prevention, they often cannot prevent the ongoing cycle of terrorist recruitment.

Prevention of recruitment to terrorism can be compared to preventive medicine, which focuses on promoting practical day-to-day approaches to support the health and well-being of individuals and communities and prevent disease, disability, and death. The fundamental approach of preventive medicine encompasses simple measures like washing hands, being careful with hygiene, immunizing the population, avoiding smoking, and getting screened for various conditions. As a result, illnesses can be prevented and people do not need expensive treatments and procedures, which saves millions of lives and dollars. Similarly, the prevention of recruitment to terrorism, by decreasing the numbers of terrorists, would not only lead directly to fewer terrorist attacks and casualties, but also to fewer resources being spent on investigating such attacks, including human and judicial resources and prison-related expenses. Furthermore, such preventive activities would lead to fewer arrests and terrorist casualties, as well as strengthening peace and harmony in societies by eliminating the escalation of conflicts.

There are increasing numbers of practices, de-radicalization programs, and programs for countering violent extremism (CVE) and preventing violent extremism (PVE). However, most of these programs focus on individuals or groups who have already been recruited or radicalized. This could be considered a late step in the prevention of terrorist recruitment, as it does not focus on individuals directly before they are radicalized and recruited.

Prevention programs targeting terrorist recruitment are also more productive than conventional police and intelligence work, simply because they reduce the risks involved when working with active terrorist organization members. More importantly, as a result of these programs, fewer individuals are being imprisoned or killed through operations, and families and communities are not being alienated or distanced from the government or law enforcement agencies. I observed consistently during my tenure in Sanliurfa, Turkey, and research activities that, even if the siblings of an arrested terrorist were not true believers in a particular terrorist ideology, the chances of their recruitment significantly increased if their loved ones had been arrested.

The advantages of the prevention of terrorist recruitment are also in line with an essential rule of countering terrorism argued by Wilkinson, namely that “governments should try and avoid over-reaction and repression by their security forces” to achieve a balanced counterterrorism strategy. From the perspectives of families and friends, counterterrorism operations might be seen as repressive and unjustifiable if their loved ones are harmed or lost, regardless of how balanced those operations are. The literature also suggests that hard-power law enforcement counterterrorism strategies should be carefully calibrated so as not to alienate populations and individuals, and they should not be excessive, discriminatory, or political. Correspondingly, Crenshaw and Roth pointed out that counterterrorism activities should be carried out under the norms of a judicial process and adhere to democratic frameworks to avoid the backlash and the emotions that can stem from disproportional interventions.

Finally, to succeed and survive, terrorist organizations are always seeking new recruits. For a successful counterterrorism policy, it is imperative that the vicious cycle of terrorist recruitment be targeted and interrupted. Preventing recruitment to terrorism should be considered the first step in countering terrorist activities. This chapter presents a road map of tactics and policies for disrupting recruitment, arguing that there is no single method when it comes to this; rather, one should follow a holistic approach that encompasses a combination of
the tools prescribed throughout this chapter, based on addressing the ideologies, demographics, and geographies and the organization, its base, and the target populations involved.

**The Concept of Terrorist Recruitment**

Historically, terrorist organizations have used different tactics to recruit new members, often based on their ideologies, locations, and objectives. From this perspective, no single, uniform recruitment process exists. However, terrorist organizations learn from each other, and there are often many similarities in how they reach out, indoctrinate, and recruit new members.

In most cases, terrorist recruitment is a never-ending process, with several different layers existing through which terrorist organizations try to extend their reach and expand their base. In fact, the life of a terrorist organization depends on its ability to reach out to new people and persuading them to join and “guarantee the next generation.” Nesser, in explaining the reliance on recruitment, points to the “culture for recruitment” among the jihadist circles and describes it as “an inherent, expansive drive to the jihadist movements,” which forces dedicated Salafi jihadists to “use all opportunities to try to recruit for their cause.”

Often, people think of the militarily trained strike forces of terrorist organizations and the ideological hardcore as those who carry out the attacks. However, there are several other structures involved. These include large state-like bureaucracies such as the state-like bureaucracy ISIS had or Hezbollah currently has, logistical and financial support units, media and propaganda units, civilian leaders assigned to control/represent different regions or structures, or simply a base, that is, people who directly or indirectly, actively or passively, support the organization ideologically, financially, or however they can, without directly being involved in armed confrontations and conflicts. In most cases, the base is where a candidate would be judged and tested before being assigned to a more serious position, as in an armed cell. Therefore, the recruitment of a terrorist organization has a broader perspective that encompasses all aspects and functions of the organization.

Terrorist recruitment is a lengthy and time-consuming process that is often well-planned and carefully conducted by the full membership of a terrorist group. For instance, Al-Qaeda produced a recruitment manual, “A Course in the Art of Recruiting,” which is a great example of how terrorist organizations emphasize the importance of recruitment by producing step-by-step field manuals to teach their members how to properly recruit by following recommended procedures.

Additionally, it should be kept in mind that a group’s inability to reach its final objective to enlist a large number of dedicated militant members should not automatically be considered an unsuccessful venture. For a variety of reasons, prospective recruits might not dedicate themselves to the group as “soldiers,” but might become part of the larger base, where they can offer support by providing resources such as finances, safe havens, and expertise.

**Key Terms: Radicalization, Recruitment, and Prevention**

There is a need to define these three terms in the light of diverse uses in the current literature, as these terms will be frequently referred to in this chapter.

**Radicalization**

Radicalization, for the purpose of this chapter, is defined as “a set of complex causal processes in which multiple factors work together to produce extremist outcomes,” leading to the assumption and acceptance of terrorist ideologies, along with the violent activities stemming from these. McCauley and Moskalenko argue that radicalization can happen at different levels;
the individual, group, and mass-public levels. The characteristics of these three levels of radicalization are used in this chapter when referring to a variety of recruitment scenarios.

It is important to acknowledge that not everybody who assumes radical ideas becomes violent or becomes a terrorist. Radicalization by itself is not exclusively the focus of this chapter but rather the socialization and mobilization towards terrorism and violence through radicalization, as the assumption of a radical ideology is the essential path to violent extremism and terrorist activity. Mark Sedgwick has been correct in arguing that the term radicalization is an ambiguous term that has created confusion among the researchers and government officials. Vergani and his colleagues categorize two different types of radicalization that result in violent extremism. They distinguish between “studies that focus on behavioral radicalization (which focuses on an individual’s engagement in violent action) and cognitive radicalization (which focuses on an individual’s adoption and internalization of violent and extremist beliefs).”

**Recruitment**

Recruitment in this chapter is referred to as the entire process by which a terrorist organization reaches out to potential new candidates and tries to persuade them to join their group, through a series of well planned, systematic, and supervised activities.

Researchers have long studied why some people get recruited to terrorist organizations, while many others in comparable circumstances do not. As explained by Hegghammer, much of the literature on recruitment falls into “one of four categories, depending on whether the focus is on supply or demand, and underlying or proximate determinants” (see Figure 1).  

**Figure 1. Typology of Analytical Approaches to Differential Recruitment**

<table>
<thead>
<tr>
<th>Underlying determinants</th>
<th>Supply</th>
<th>Demand</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Recruit attributes</td>
<td>Group attributes</td>
</tr>
<tr>
<td>Proximate determinants</td>
<td>Networks, socialization</td>
<td>Recruiter tactics</td>
</tr>
</tbody>
</table>

While numerous researchers have studied various aspects of terrorist recruitment, such as the demographics of recruits or their psychological profiles, this chapter examines the process itself.

**Prevention**

Prevention is the action of stopping something from happening. In this chapter, the term prevention of recruitment is used to mean planned, systematic, and holistic action taken to stop a prospective recruit from joining a terrorist organization. Prevention can be applied at any stage of the recruitment process. In the context of this chapter, the term prevention does not refer to hindering terrorist attacks or other terrorist actions, but rather to preventing terrorist recruitment.

The majority of the research conducted under the notion of prevention falls under “terrorism prevention policy and programs” that aim “to reduce the risk of terrorism by applying tools and approaches other than the traditional law enforcement and criminal justice tools of arrest, prosecution, and incarceration.” This chapter on the prevention of terrorist recruitment covers parts of these efforts; however, its focus is solely on the prevention of terrorist recruitment, which should be considered as a subcategory of the broader “terrorism prevention policy and programs.”
The Attack-Exposure-Propaganda-Recruitment Continuum

Beyond their ideologies, terrorist organizations thrive on four important elements to survive. Essentially, these steps follow each other, each kick-starting the next part of the process through a vicious cycle, constantly contributing to the survival of terrorist organizations (see Figure 2).

Terrorist attacks are inherently designed as communication tools used to spread fear among the populace and convey a message through violence. This is one of the main reasons for why, in Schmid and Jongman’s groundbreaking analysis of the discourse of terrorism definitions, which examined the frequency of terms in 109 definitions, ‘violence and force’ had the highest frequency, at 83.5 percent, and ‘fear and terror’ emphasized the third-highest frequency, at 51 percent.17

As communication strategies, terrorist attacks first aim to present terrorist organizations as more powerful and sophisticated than they actually are. Second, attacks are carried out to hijack media coverage and help spread their messages in the aftermath of an attack. Terrorist attacks may dominate for a short while the world agenda, leading to intense publicity through excessive media coverage (and now through social media as well), which translates into mass propaganda. This free media coverage enables the terrorist organization in question to recruit more members. As early as 1975, Brian Jenkins, noted, “Terrorists want a lot of people watching, not a lot of people dead.”18

Free media coverage and propaganda spread through terrorist attacks, in a sense, catalyze the base of a terrorist organization. They send the message that a group is powerful; in the words of a terrorist I interviewed in the past, “boiling the blood of their base to mobilize them,” and affording them opportunities to reach out to new people.

Gaining publicity through terrorist attacks has historically been one of the main objectives of terrorist organizations. In fact, the British Prime Minister Margaret Thatcher, discussing the 1985 Trans World Airlines hijacking, urged democratic nations “to find ways to starve the terrorist and the hijacker of the oxygen of publicity on which they depend,” to stop this cycle.19

In 1989, the doyen terrorism studies scholar Alex Schmid, realizing the role of media in this cycle, simply warned editors of mass media not to be “the terrorists’ accomplices”.20

Figure 2. Terrorist Organization Attack and Recruitment Cycle
Similarly, addressing the issue of terrorist publicity and media, another leading terrorism studies scholar, Dr. Bruce Hoffman, stated:

“The modern news media, as the principal conduit of information about such acts, thus play a vital part in the terrorists’ calculus. Indeed, without the media’s coverage, the act’s impact is arguably wasted, remaining narrowly confined to the immediate victim(s) of the attack rather than reaching the wider ‘target audience’ at whom the terrorists’ violence is actually aimed. Only by spreading the terror and outrage to a much larger audience can the terrorists gain the maximum potential leverage that they need to effect fundamental political change.”

The coverage of a terrorist attack by the media gives a terrorist organization free TV airtime and print media coverage. Thus, the intended reaching out automatically occurs, and the organization may be able to start to recruit more members or reach out to new people to recruit. In the mind of an extremist and radicalized believer in the ideology of a terrorist organization, seeing coverage of a terrorist attack in the media can often become a spark and starting point, prompting that person to decide, “I should do something, too.” This was explained to me by a terrorist during an interrogation I held on how he decided to join a particular terrorist organization.

Therefore, being aware of how terrorists use ongoing attacks to prove that they are alive and powerful and to ensure a flow of recruitment is one of the most essential steps in preventing recruitment. It is possible to design strategies to intervene in this vicious cycle at any point in order to weaken the recruitment process.

Organizational Structures of Terrorist Groups and Recruitment

Terrorist organizations have different structures, based on their size, ideology, geographical location(s), operations, and objectives to achieve long-term success. Structures can also be fluid, as terrorist organizations usually respond to challenges by modifying their structures or adopting new techniques to maintain efficiency and “protect against infiltration and threats.”

For instance, Kilberg identified four basic terrorist structures, based on a study of 254 groups (“market, all-channel, hub-spoke, and bureaucracy”). Understanding terrorist structures is essential, particularly when it comes to dealing with terrorist recruitment and attacks. Terrorist structures and hierarchies essentially reveal how groups operate daily, who communicates with whom, and how tasks are delegated among members. More importantly, the ways in which terrorist propaganda activities are carried out can lead to increased recruitment. Who oversees recruitment activities and where these take place are important aspects of the terrorist human resource acquisition process, and these can be understood only if organizational structures are exposed. Another piece of critical information, from the perspective of prevention, is understanding “who is (or can be) in touch with whom” in such an organization.

The objective of this chapter is not to study the structure of terrorist organizations; however, we are going to look at a few sample structures to illustrate how recruitment is conducted.

Before the ISIS caliphate was established, its senior members planned the future structure of the organization, because they knew success would depend on it, not only for ensuring its efficiency, but also for protecting the security of its members and organizations. With this in mind, Samir Abd Muhammad al-Khlifawi (a.k.a., Haji Bakr), a former Iraqi colonel in the intelligence service of Saddam Hussein, drew up a plan for the structure of ISIS, which constituted the first version of its organizational structure.
The caliphate was established in 2014, and as ISIS started to control large areas, its structure evolved into the following hierarchy, encompassing several activities beyond its military operations. The ISIS structure reveals that there are many layers of hierarchies involving different tasks, from media to sharia commissions to security. When ISIS functioned as a state-like organization from 2014 until 2018, most of its structures were open to the public, other than its security apparatus. Members were usually identified with their tasks. However, after its defeat, ISIS evolved into an insurgency group, and its structure was rapidly updated to face the consequent realities and necessities.

The Turkish terrorist organization Revolutionary People’s Liberation Party/Front (DHKP/C), had a structure dividing the armed and unarmed wings very carefully, not only controlling the communications between these two wings, but also keeping the armed wing underground for their own security (see Figure 3). These two wings were called “unarmed, political, or legal” vs. “armed, military, or illegal” to designate the allocation of tasks. This structure is essential to understanding the typical activities of a terrorist organization.

What is seen on the left side of the schematic in Figure 3 is the face of the terrorist organization, whose members freely operate above ground through legal means, enjoying freedoms, such as free use of the media, freedom of speech, freedom of assembly, and the right to establish foundations and associations, university and high school activities and clubs, workers’ and officers’ unions, and neighborhood clubs, in an effort to produce legal fronts to attract people to their activities. This can be done for a variety of objectives including recruitment, expanding the base, disseminating propaganda, and providing safe havens. The strategy of having larger bodies legally operating in a free society by using the constitutionally

Figure 3. Sample Structure of the DHKP/C, a leftist Terrorist organization based in Turkey
provided rights and freedoms with less security and secrecy is to have the means to reach out to the public and to create operational spaces for armed groups when necessary, through the coordination of the higher command with people in charge of different units.

One of the most important tasks of the unarmed wing has always been the recruitment of new members. Because this wing operates freely in public within assigned units, it has always been tasked with recruitment, in addition to other assigned duties. For example, the media wing produces journals or newspapers for the organization, while trying to reach out to potential new recruits through its day-to-day activities. Because the members of the unarmed group are tasked with recruitment, organization members always meet and interact with newcomers in their unit until they are fully vetted and evaluated, at which point a new recruit is assigned to another unit, based on their education, skill sets, character traits, and dedication. Therefore, the unarmed wing is essentially the base of the terrorist organization, where most recruitment activities are conducted, along with other tasks.

The most important aspect of this unit from the perspective of recruitment is the fact that no new member would be directly assigned to the military or armed wing of the terrorist organization before spending considerable time in the unarmed wing. This is done not only to prove their dedication and trustworthiness, but also to establish a foundation for continuous ideological indoctrination. Reality, the flow of new members from the unarmed wing to the armed wing is a very slow process. Assignments happen based on the needs of the armed wing and the qualities of the new recruits, who are kept in the unarmed wing for as long as possible.

The flow of new recruits to the armed wing depends upon several factors. Among these are the newcomer’s qualifications, ideological indoctrination and commitment, health and physical strength, skill sets, as well as secrecy issues – and unforeseen events like being “burned” (uncovered by law enforcement and intelligence) or being subject to situations such as becoming vulnerable to arrest or undergoing a prison sentence after a trial.

Finally, once a member of the unarmed group is assigned or passed to an armed unit, the new member usually goes through military training and is assigned to a new location, typically a new city or country where he or she is not known to members of the public.

This scheme and the slow flow of new recruits from the unarmed to the armed wing of a terrorist organization provides (from the perspective of the prevention of terrorist recruitment) ample opportunities to intervene in the recruitment process while it is happening out in the open before someone is passed on to the armed wing. In an armed wing, the rules of secrecy are substantially stricter, and members, in most cases, live in carefully structured cells, which makes it more challenging and difficult for the law enforcement and intelligence communities to penetrate the organization.

While Figure 3 does not represent the structures of all terrorist organizations, most terrorist groups apply similar rules or tactics, and often they do not immediately assign new members to more professional and secretive armed units. An exception to this rule would be cases of armed group members with previous and trusted connections -which happened in the past with the DHKP/C, Al-Qaeda, and ISIS - based on mutual trust and the needs of the groups or stemming from the exodus of members to the ISIS caliphate, which represented a state-like organization handling tens of thousands of newcomers.

**Terrorist Recruitment and Radicalization Process**

When I first started to work in counterterrorism in 1995 in Ankara, Turkey, I immediately realized that terrorist organizations were recruiting most of the siblings and close friends of the suspects we were arresting. In fact, I realized that the driving factor for terrorist recruitment was often not the ideology or the justifications of the terrorist organization, but rather, the prior connections and emotional attachments with the family and friends who had been arrested. Considering what I was experiencing and observing, I tried to understand why individuals were
becoming terrorists and engaging in extremist behaviors. Like many other researchers, I believed that knowledge of the terrorist recruitment methods would be key to successfully countering terrorism and preventing recruitment.

During my twenty-year long career in counterterrorism, I collected data for the terrorist recruitment prevention program called “Preventing Terrorist Recruitment through Early Intervention by Involving Families,” which I established in Sanliurfa, Turkey, between 2010 and 2014. As the chief of counterterrorism, I developed the descriptive scheme described below for the “terrorist recruitment and radicalization process.” It is imperative to note that the following model represents face-to-face and direct recruitment methods. Radicalization and recruitment through social media and the internet will be discussed separately.

I studied terrorist recruitment methods, particularly with youth, and investigated how people were being approached by different terrorist organizations and what tactics were being used, beginning with initial connections and proceeding over the years towards membership. Both my master’s thesis and PhD dissertation focused on terrorist recruitment and how to deal with it in the long run.

During my interviews with terrorists who were members of ISIS, Al-Qaeda, Hezbollah, the Kurdistan Workers’ Party (PKK), the DHKP/C, the Liberation Army of the Workers and Peasants of Turkey (TIKKO), and many other organizations, and the case I recorded, I realized that there were often similar patterns in terrorist recruitment and the radicalization process, regardless of the organization or ideology.

It is essential to understand that each step of the “terrorist recruitment and radicalization process” is an opportunity to intervene and to reverse the course of the process. It is only possible to successfully prevent the recruitment of new members to a terrorist organization if the authorities understand how the recruitment process works.

Terrorist organizations tend to monitor and supervise recruitment activities closely. As a general rule and principle, almost all terrorist organizations require their recruiters to report each of the recruiting steps to their superiors before taking any action. These reports may include how the recruiter knows the prospective subject, their background and biography, qualifications, education, work, ideology, doctrinal commitment, and special skills. Often, during terrorist cell operations, authorities recover hundreds of pages of handwritten or digital reports detailing the above elements for different subjects, written by the recruiters and detailing the progress they were making. The DHKP/C and Hezbollah were particularly very keen on producing such reports, and the recruiters’ superiors would pass the reports to their leaders. For example, the Turkish National Police confiscated the archive of Hezbollah in July 1999, which consisted of 41 hard drives, two laptops, and over 300 CD-ROMs, with over 133,000 pages of documents, which included internal communications, financial reports, the biographies of thousands of prospective recruits, and reports about the recruiters’ progress.

The Terrorist Recruitment and Radicalization Process

I defined the following stages of the terrorist recruitment and radicalization processes based on my experience as an active law enforcement counterterrorism officer over twenty years and on the basis of my counterterrorism research activities, detailing how and through which phases a person is recruited into a terrorist group. These stages constitute essential milestones in becoming a member of a terrorist group and identify the activities by which authorities can intervene to interrupt the process, provided they are aware of how each step works. Therefore, I will detail and explain each stage carefully, presenting its main theme, objectives, and possible activities.

1. Identifying the candidate.
2. Initiating contact (if contact didn’t exist already).
4. Advancing friendship and trust, introducing ideological indoctrination, and playing to emotions.
5. Isolating the recruit and advancing indoctrination to networking with other terrorists and associations.
6. Reinforcing the assumption of a new identity.
7. Introducing the recruit to simple terrorist activities such as demonstrations and social media posts.
8. Assigning candidates to different parts of the terrorist organization.

**Identifying the Candidate**

The identification of the candidate is the first step in the recruitment process. There are two types of recruitment based on the policies and needs of a terrorist organization. The first type is “opportunistic recruitment,” where recruiters try to recruit people whom they already know, with whom they already have connections, or with whom they can connect through a variety of means.

The key factors enabling the identification of a candidate at this stage include prior connections, education and intellectual capacity, demographic characteristics, the type of neighborhood, and whether the prospect has someone associated with a terrorist organization in his or her family or circle of friends.

In “opportunistic recruitment,” terrorist organizations seek to increase their membership and base and will welcome anyone who can be securely recruited and is trusted. For instance, Al-Qaeda, in its recruitment manual29 “A Course in the Art of Recruiting,” provides a pathway to “opportunistic recruitment.” This is the general practice for most terrorist organizations. However, this type of recruitment should never be understood as welcoming everyone into a terrorist organization, because terrorist organizations have different sets of rules to vet newcomers in an effort to ensure their secrecy and weed out possible informants or unwanted characters. For example, Al-Qaeda strongly advised against recruiting the following types of people: cowards, excessively talkative people, people who entertained hostile ideas toward the Mujahideen, stingy people, and loners.

The second type of terrorist recruitment is targeted recruitment through “talent spotting.”31 In targeted recruitment, terrorist organizations tend to seek out people with special talents and qualities who can be assigned to work in certain units or areas that call for qualified members to carry out the assigned tasks, such as producing sophisticated explosives or try their hand at developing chemical and biological weapons. To give an example: in the 1970s, the Provisional Irish Republican Army (PIRA), according to Mia Bloom, “trail blazed this innovation of talent spotting during the Troubles (1970s) in which the organization visited college campuses and sought out potential recruits with advanced educational degrees (especially in the fields of math, chemistry, and engineering - all disciplines that aided in the development and improvement of IRA explosives).”32

Similarly, ISIS leader Abu Bakr al-Baghdadi, after the caliphate was established in 2014, issued a call to his followers via an audio message that was later published in the first issue of the ISIS journal *Dabiq*. Al-Baghdadi appealed to skilled and qualified Muslims to support ISIS by inviting them to his caliphate. He appealed to “Muslim doctors, engineers, scholars, and specialists” in his speech, stating:

“We make a special call to the scholars, *fuqaha’* [experts in Islamic jurisprudence], and callers, especially the judges, as well as people with military, administrative, and service expertise, and medical doctors and engineers of all different specializations and fields. We call them and remind
them to fear Allah, for their emigration is *wajib 'ayni* [an individual obligation], so that they can answer the dire need of the Muslims for them. People are ignorant of their religion and they thirst for those who can teach them and help them understand it. So, fear Allah, O slaves of Allah.”

I also personally observed several cases where different terrorist organizations made special efforts to recruit people based on their qualifications, particularly at universities and at high school levels. In most cases, the recruitment of certain high-profile students led to an increase in the number of new recruits and gave the organization a stronger foothold in the institutions the young recruits were attending.

**Initiating Contact**

At this stage, the recruiter initiates contact with his or her subject if it did not already pre-exist, or the recruiter might seek an intentional and focused connection with the subject. Obviously, there is no need to establish initial contact with a target subject if the recruiter already has a prior connection through family ties or friendships. However, in many cases, terrorist recruiters use a variety of tactics to establish sites to which they can attract new subjects for recruitment purposes, such as cultural centers, bookstores, cafes, youth centers, music concerts, after-class study sessions, and free courses.

Al-Qaeda considers the first two steps in this model to be the first stage of its recruitment process, which is labeled “Getting Acquainted and Choosing”; it instructs its members to “look around yourself carefully, maybe you will find a Mujahid you hadn’t recognized before. Ponder on all of the people and look for a Mujahid amongst them.”

**Building Rapport and Friendship**

Usually, recruiters seek ways to spend time with their subjects. At this stage, we often observe increased social activities between the subject and recruiter, including attending after-school activities, participating in weekend and evening gatherings, going to movies, spending time at malls, and taking long walks. Typically, the involvement of other players or terrorist-related entities is not observed at this stage. Recruiters usually focus on ascertaining whether or not they can trust their subjects and if it is worth continuing to work on them.

Generally, recruiters, as with most terrorist organizations, are required at this point to report their progress in their recruitment efforts. In most cases, they must make a detailed report in order to get feedback and directions from their peers and unit leaders. For example, the Al-Qaeda recruitment manual names this stage as “Getting Close (or Approaching)” and builds it on two axes or hubs: “[T]he first one is getting close through daily work (routines) and the second one is getting close through weekly work.” Al-Qaeda urges its recruiters to invite their subjects to meals and give them gifts to become closer to them. Furthermore, the manual provides a questionnaire for assessing whether a candidate is suitable for the next level of the recruitment process, which includes questions such as:

1. “Is he eager to see you?”
2. Does he talk with you about his private affairs and his hobbies?
3. Does he ask you to help fulfill his needs concerning Allah (SWT)?
4. Does he follow your orders?
5. Has he told you that he loves you (for Allah)?
6. Has your fondness for him increased?
7. Does he love to spend a lot of time with you?
8. Does he accept your advice and respect your opinion?”
**Advancing Friendship and Trust, Introducing Ideological Indoctrination, and Playing to Emotions**

Recruiters, after ensuring that they can trust their subject and after receiving approval from the organization, start to deepen their friendship with the prospect, playing to the person’s emotions by fostering the idea that they are close friends, even sharing a brotherly or sisterly type of affection. The objective is to make subjects believe that the recruiter is their best friend and that there is complete trust between them, which is destined to lead to an emotional bond.

At this stage, the primary objective is to enhance rapport and trust between the recruiter and the subject, while slowly introducing the organization’s ideology without mentioning the organization. Thus, the final goal at this stage is to build the utmost trust and affection between the parties, for two essential reasons. The first is that the trust and confidence between the parties help subjects to believe what they are being told by the recruiter. The second is that the connection between the parties will eventually ensure that the targeted subject will not be able to say “no” or “deny the requests” of the recruiter, due to the affection that has grown between them. This is done by recruiting the subject in such a way as not to lose the friendship, which constitutes the essential foundation of terrorist recruitment. When the time is right at the end of the recruitment process, the new recruit will be locked into that friendship. Even if the new recruit has some doubts, the emotional ties and the affection established will help the recruiter to proceed to the next stages.

One can often observe the start of ideological indoctrination at this stage. While the recruiters and subjects have sometimes talked about the ideologies of terrorist organizations and the justifications for their existence, at this stage, the indoctrination of the subjects becomes systematic, and the recruiters try to make them true believers in their ideology or at least the non-violent version of it. Nevertheless, in most cases, terrorist organizations and their violent activities are not introduced nor mentioned during this stage; rather, the general concepts of terrorist ideologies are introduced.

For leftist terrorist organizations, indoctrination involves Marxist ideology and thought; for the Salafi jihadist terrorist organizations, the discussion revolves around Salafism and Wahhabism without reference to the terrorist organizations. For example, Al-Qaeda asked its recruiters at this stage not imply to their subjects that “Jihad is al-Qaida.”

In general, I did not observe the introduction of justifications of terrorist violence at this point during my past interactions with terrorists nor did I find it in my research. However, depending on the ideological commitment and readiness of a subject, a recruiter could start to talk about the actions of the terrorist group and their justifications to accelerate the recruitment process. Basically, each subject is evaluated individually on a case-by-case basis, and the actions of the recruiters are adjusted accordingly.

Al-Qaeda calls this stage “The Awakening of Iman” and advises its recruiters not to

> “show the candidate any jihadi videos, audios, etc. except when his Iman (faith) is at a high level, and when he is in a state of tranquility in order to have the best effect on him and on his heart. And don’t let him listen to anything (i.e. videos or audios) when he is bothered or sad because it will be of no benefit for him.”

**Isolating the Recruited Person and Advancing Indoctrination to Networking with other Terrorists and Associations**

Isolating the recruit and advancing the indoctrination process to networking with other terrorists and associations constitutes the most important and intense phase of the terrorist recruitment process. During this stage, recruiters do their best to make sure that their subjects
become true believers in the organization’s ideology. During this process, there is often increased activity of reading together, discussing ideological materials, summarizing the material being read, watching videos, and exchanging books related to the ideology of the particular terrorist organization.

Another important aspect of this stage is the initiation of the “isolation phase.” This is when the recruiter ensures that the prospective recruit will distance himself or herself from previous social settings and start to associate with the recruiter’s network. In addition, isolation often takes place through a lifestyle change based on the newly acquired ideology. The recruit is introduced to other members of the terrorist network, and often those members put extra efforts into having the new person feel at ease and comfortable among them by being extremely nice and compassionate. This approach seems to work very well with young people, because they want to spend more time with their new inner circle of friends. Al-Qaeda emphasizes to its recruiters the importance of networking, with the following advice, “You should know, my dear brother, that the best way to inculcate the concepts is to do it in a group, and this is the opinion of the people who master this art (recruiting).”

Isolating a new recruit is essential to ensure his or her assumption of a new identity and is the pathway to radicalization. At this stage, the subjects are expected to read and associate themselves exclusively with the literature of the terrorist organizations they are joining. These materials include the organization’s books, journals, videos, audio recordings, and social media accounts. The recruits also cut their ties with their former social circles and friends, avoiding places they used to frequent, and adopt a lifestyle that distances them from other ideological and social groups.

Alexandra Stein, in her book *Terror, Love and Brainwashing*, describes this situation as setting up “the conditions for a later rearrangement of the recruit’s close relationships” by getting the prospective recruits into the organization’s sphere of influence. Stein further elaborates on the next step, in which the organization can begin the isolation project and start to position itself as the primary emotional and cognitive resource for the recruit – becoming the new, and eventually the only, safe haven. There is a three-fold process in setting the stage for the creation of an attachment bond to the group: gaining access to the recruit through initial contact, positioning the group as a newly perceived safe haven and beginning to detach the recruit from prior attachments. Propaganda is the ideological tool wielded to accomplish this. During this stage, the candidates are expected not to get involved with the teachings and literature of other ideological traditions and to not communicate or discuss these ideologies.

**Figure 4. Recruitment Approaches used, Depending on the Environment**

![Recruitment Approaches](image-url)
with others, including family members; this is particularly true for the new members. The motive here is to limit access to the counterpropaganda and ideological approaches of other groups by isolating new recruits from the outside world, a tactic also used by cults. Indoctrination is used to reduce the risk of defection to competing rebel groups.

This mindset and the tradition of controlling new and prospective recruits create a high barrier to the prevention of terrorist recruitment. Al-Qaeda calls this stage “The Stage of Planting Concepts” and advises recruiters to have their subjects do the following to reinforce their identities:

- “A book called “Questions and Doubts regarding the Mujahideen.” The candidate must read this book because it is very beneficial and will help him to protect himself.
- The candidate should see all the meetings with our ummah’s wise sheikh Al-Zawahiri because these meetings revolve around the Jihadi ideas.
- Let him watch all the productions of Al Sahab, Al Furqan, Al-Maghrib Al Islami, and Chechnya. However, make sure you show him these in stages, and select the best ones of their videos.”

Leftist terrorist organizations used to make great efforts to ensure that their subjects would be fully indoctrinated during this stage. Back in 1998, a DHKP/C member told me how he was forced to read 300 pages a day, summarize what he understood and discuss it with his peers for ninety days during his summer break. Similarly, ISIS set up ideological training camps - often linked to military training - and produced a collection of textbook-like manuals consisting of over 10,000 pages and made sure its members studied them during their training.

As already mentioned, this stage marks the beginning of lifestyle changes based on the terrorist group and its ideology. The prospective recruits start to distance themselves from their former networks; they may change their attire based on the newly assumed ideology, such as growing a beard without a mustache and, for Salafi jihadist terrorist groups, wearing “short pants (above the ankles) and knee-long shirts.”

Christianne Boudreau from Calgary, Canada, the mother of Damian Clairmont, who joined Jabhat al-Nusra in 2013, described this stage, mentioning she “noticed a change in her son. If he was visiting and his new friends called, he would only answer the phone outside. He wouldn’t eat with the family if there was wine on the table. He told his mother that women should be taken care of by men and that it was acceptable to have more than one wife.”

At this stage, also, the subjects interact, socialize, and associate with known terrorist front entities. These are essentially places, operating under regional or ideological names that do not reveal their ideological affiliation - places which serve as common ground and meeting spots for the terrorists and young people, designed to attract new people run by the terrorist organization. They are such sites as foundations, associations, bookstores, charities, Internet cafes, study groups, tea houses, music and dance courses, sports academies, language centers, and other places where known terrorist members are present while prospective recruits spend time there.

Kruglanski describes this networking and socialization stage as involving “the presence of an ideological component that identifies involvement in terrorism as an appropriate means to gain (or regain) a lost sense of significance, followed by a process of socialization and implementation.”

Similarly, Jensen portrays this process by referring to social identity theories of radicalization, which suggest that “increased group cohesion can produce dangerous group biases, such as group polarization; groupthink; in-group/out-group bias; diffusion of responsibility; and rule compliance that lead members to adopt increasingly extreme beliefs or engage in extremist behaviors.”
Nesser describes this stage by noting that,

“analysis suggests the existence of a ‘culture for recruitment,’ which implies that recruits are socialized by friends and acquaintances in militant milieus, mainly through religious and political discussions, and ‘team-building’ activities initiated by the terrorist cell leaders. Team building often involves physical training, weapons training/paintball, watching propaganda movies, and attending the sermons of radical clerics.”

The role played by socialization in the process of recruitment is seen in the following example: ISIS set up a coffee/teahouse called “the Islam Teahouse” in Adiyaman, Turkey, in the center of the city to serve as a hub where prospective Turkish ISIS members could spend time with other ISIS members. Many other people simply felt that the teahouse was attractive because of its name and went there. It was reported that around fifty people visited and spent time in this teahouse daily, and by 2015 it had facilitated the recruitment of around 300 Turkish ISIS members, including the terrorists behind the 2015 Suruc and Ankara suicide attacks, which killed 143 people and wounded over 600.

Similarly, Al-Qaeda organized picnics where prospective recruits, new members, and experienced members were tasked with meeting newcomers by gathering in the countryside to spend time together. Sometimes this was done with the participation of the members’ families to establish closer bonds and to welcome the new members. The leader of Al-Qaeda in Turkey, Habib Aktas, reportedly arranged several picnics in 2004 to motivate Turkish Al-Qaeda members.

**Reinforcing the Assumption of a New Identity**

Terrorist candidates, at this stage, realize that they have fully associated themselves with the group and assumed the identity and accepted terrorist teachings imposed by the recruiter and by their new network of associates. It should be understood that the isolation of the new recruit continues during this stage, as the newcomer is carefully observed by the recruiter and the network.

This is the stage where the recruit is offered the chance to become an official member of the terrorist organization. Based on my personal observations and research, if subjects make it through this step, it becomes very difficult for them to disassociate themselves from the group. This is often because of the close friendships and bonds developed and due to the ideological indoctrination. If a subject has passed the prior steps, it usually means that he or she will formally become a new member of the organization.

This stage is Al-Qaeda’s last stage of the recruitment process, which it calls “The Establishment of the Brigade”: “During this stage, the brother [candidate] will be: Convinced by the most important concepts of the jihadi methodology with a real desire to perform jihad.”

**Introducing the Recruit to Simple Terrorist Activities Such as Demonstrations and Social Media Posts**

The new recruits are welcomed into the group and assigned, in most cases, to a local sector of the terrorist organization. This depends on the needs of the group and the qualifications of the new members, but they are often sent to the unarmed wing of the group for further testing and observation, to give them a chance to acquire more experience. At this stage, the candidate feels like part of the group and understands that he or she is now inside the terrorist organization. The organization constitutes an inner circle where the new member feels welcome and enjoys being with his or her new friends. There is also a sense of an outer group,
a presumed enemy, which may consist of rival groups, governments, and adherents to other ideologies.60

During this stage, the affiliations with the group are usually not visible to the outside world. If the group would like to reinforce the new member’s identity and affiliation with the group, he or she will be asked to carry out seemingly innocent and harmless activities, such as being part of a demonstration, distributing pamphlets and booklets, writing graffiti, transporting books or funds, or engaging in other activities which would not be openly deemed illegal. This stage serves as a pathway to becoming a trusted member and affords opportunities for new recruits to prove themselves. I have often observed that young recruits would be charged up emotionally at this stage, eager to carry out the activities they were assigned to do.

There is an additional reason why new members are asked or encouraged to carry out these simple terrorist tasks. Through these activities, two messages are instilled in the mind of a new terrorist. The first is that there is excitement and pride involved in proving oneself, strengthening one’s ties to the group, and carrying out an attack with fellow members for an ideological cause. Salafi jihadist groups also introduce these activities as good deeds for the cause of their religion, which is deemed to help the participants to earn a place in paradise. Leftist organizations have a similar mindset, encouraging their new members to join in simple attacks and praising their courage and bravery despite them being newcomers. The approval of the inner group and close friends gained through simple terrorist activities influences the mindset of the new member and strengthens the idea that he or she is part of the group and is welcomed and accepted.

The second reason for asking new members to carry out simple attacks is to incriminate them in the eyes of the judiciary or law enforcement, simply saying or implying that “now that you committed a crime, you have to stick with us, and we will protect you as a member and make sure that you are not caught or imprisoned.” At this stage, the new member often already assumes the government forces are an enemy, believes that the police are after him or her, and feels the need to stick with the group to be safe.

Assigning Candidates to Different Parts of the Terrorist Organization

At this final stage of the recruitment process, the candidates have proven themselves and are ready to be assigned to different parts of the organization. The assignments are usually done on a case-by-case basis, and different factors are taken into consideration before a newly recruited terrorist is relocated, which includes issues such as whether candidates are about to graduate from college or high school, whether they can cut their ties with their family, whether they have enough courage to live abroad under stressful conditions, and whether they possess the desire or physical strength to go through rigorous military-style training.

It is common to observe certain behaviors if a newly recruited terrorist is going to be assigned abroad or relocate. These include going on a shopping spree to get ready for the new assignment, buying gifts for friends or family members, interacting with close family members (which, from the terrorist’s perspective, is meant as a farewell), emptying bank accounts, spending money to the maximum limits of credit cards, or, for more critical assignments, suddenly going missing.

In general, a newly recruited member is not sent abroad directly. Rather, under normal circumstances, a newcomer is assigned to a local area to work in an unarmed unit, so that more senior members can observe, get to know, and test the recruit over time, and produce reports about his or her qualities and characteristics. Unless the terrorist organization is in a rush to assign more manpower to its armed division, it usually takes over a year for a new member to be relocated.
Terrorists are often relocated or assigned abroad if a member is deemed to be in jeopardy of being arrested because of an ongoing police investigation or counterterrorism-operation, or if a member’s connection to the terrorist organization and their activities are somewhat revealed. Furthermore, terrorist organizations usually relocate their critical cadres and local leaderships constantly, in order to try to hide their identities and keep their faces from becoming familiar to local authorities.

Prevention of Recruitment

Preventing terrorism and terrorist recruitment is a delicate practice that requires a professional approach and the involvement of a combination of well-informed and educated officers, specialists, experts, volunteers, and others. Preventing recruitment before a prospective recruit is completely assimilated should be considered a matter of communication and outreach, rather than one for law enforcement or for an intelligence operation. The objective of preventing terrorist recruitment is not to prosecute those who are being approached by terrorist recruiters, but rather to save them from being pulled into a terrorist group to begin with.

Therefore, for a successful intervention and prevention program, the people who are intervening must understand the delicacy and sensitivity of what they are doing, should have a deep understanding of the terrorist organization they are dealing with, must be able to evaluate the psychology of their subjects, and should know how to approach vulnerable populations in order to be able to open communication channels. While not everyone involved in prevention activities needs to have the same depth of knowledge, the managers and individuals who meet and interact with the vulnerable populations should be equipped to handle a variety of scenarios, along with a well-established understanding of how to communicate with the individuals they are approaching. There are no pre-set techniques when it comes to the prevention of terrorist recruitment; rather, a holistic approach encompassing a variety of techniques based on the subjects and conditions should be adopted.

Key Concepts and Qualifications

Understanding the Terrorist Organization in Question

One of the most important qualifications of the individuals who are part of an intervention and prevention team is an understanding of the terrorist organization they are dealing with, not only locally, in terms of its jurisdictions and neighborhoods, but also globally, since many contemporary terrorist organizations act in harmony and are quickly affected by the actions of their peers abroad. Understanding a terrorist organization should cover the following elements, because each plays a key role in the daily lives of an organization and its members:

- The ideology of the terrorist organization, including its historical evolution and belief systems, and sensitive matters which may have significant meaning for the followers of that ideology.
- The history of the terrorist organization and its existing state of affairs, including its past activities in a region.
- The structure of the terrorist organization, particularly regarding recruitment activities, the movement of recruiters, the involvement of the base, and the leadership of the organization in a given region and the departments they head.
- The tactics of the group in question, from recruitment to propaganda, including how it carries out terrorist attacks and its weapons and explosives of choice.
- Social media outreach, and other communication mediums which the group uses to communicate and disseminate propaganda.
• Recruitment and training schemes, outreach arrangements, and the front operations the organization uses to pull people into its circle.
• The base of the terrorist group in question, including who supports the group in a given jurisdiction, whether there are hot spots for the group and its ideology in the region, how it interacts with nearby groups, whether its base provides safe havens and financial support, and so forth.
• Local trends and customs observed by members of the group.
• Analysis of any of the vulnerable local populations who could be directly or indirectly subject to terrorist propaganda and recruitment activities.

Understanding the Demographics
An analysis of the regional demographics that terrorist organizations target is essential for the prevention of terrorist recruitment. The prevention team should have a good sense of education levels, financial and employment-related facts, family structures, family size and age distribution, the locations and roles of schools and universities, health facilities, libraries, and related important facts covering the region in question. These sociological factors often deeply affect the psychology of individuals vulnerable to terrorist recruitment.

Another important factor is knowing and understanding the religion, culture, and values of the people of the region, respecting people’s values when interacting with them, and never discounting or disrespecting their belief systems or religions. People tend to become alienated when their values are disregarded, and such a move could easily shut down the communication channels between those who are trying to prevent terrorist recruitment and their subjects.

An Awareness of Terrorist Organizations’ Justifications
Terrorist organizations employ a number of arguments and justifications to explain and rationalize their activities, particularly their use of violence. Often, terrorists are taught about these arguments in advance and supplied with a variety of scenarios for how and when to apply them, some of which are also used during the recruitment cycle. These may be publicly recognized rationales which people other than terrorists may support, such as appeals relating to economic inequalities, corruption, harsh punishment, torture, injustice, or any other social or economic problems that plague the society and have a particular resonance with a terrorist ideology.

For example, leftist terrorist organizations might blame capitalism for economic problems and the injustices and inequalities in societies, and Salafi-Jihadist terrorist organizations, particularly Al-Qaeda, argue that the House of Islam is being subjected to invasion by the US military because they have military bases in Saudi Arabia, which gives the organization the authority and right to fight back against the Americans. It is essential that the intervention and prevention team members be aware of the justifications and arguments terrorist organizations adopt, so they can be ready to talk about them. However, teams should not unnecessarily raise these topics in conversations, so as to avoid conflict and alienation when they are trying to build rapport and connections with vulnerable populations.

The Base
A terrorist base basically consists of a segment of a regional population who, at the very least, adhere to an ideology in sympathy with that of a terrorist organization, such as Salafism versus Salafi-jihadism, and who may condone some of the activities of the terrorist organization.
Some may only approve in theory but not take direct action, while others may support the activities of a terrorist organization by various means, direct or indirect, active or passive, including providing financial or logistical support, safe havens, medical aid, and means of communication (such as acting as couriers), or providing other types of support that do not directly involve open illegal activity. The presence of a terrorist base is essential for a terrorist group because operating in a region with a strong base is a lot easier and safer for the terrorist group.

In addition, bases are often breeding grounds for terrorist organizations, offering them sites and networks that enable them to reach out to individuals, particularly youth, for recruitment purposes. My dissertation research, covering various terrorist groups in Turkey, indicated that previous interactions with terrorist organizations significantly increased the chance of being recruited, especially if the family of a targeted subject was within the base of a terrorist organization. This, in turn, significantly increased the rate of recruitment into terrorist organizations. My findings also revealed that teenagers were more vulnerable to terrorist recruitment if they or their family members shared an ideology with a terrorist organization or had previous interactions with it.

**Hot Spots**

Terrorist organizations use a variety of locations that are fully or partially open to the public, which serve as fronts for different purposes. While the primary role of these fronts may vary based on the region, the needs of an organization, and its ideology, these fronts often serve as places where members of a terrorist organization can interact with other people to make initial connections and identify potential candidates for recruitment. Such places are not directly identified with their affiliations with a terrorist organization but are often legal establishments where people can carry out legitimate activities freely and openly, such as:

- associations and foundations
- bookstores
- cafes, coffee or tea houses
- internet cafes
- media centers
- mosques, masjids (prayer houses)
- sports complexes, gyms, or workout centers
- music clubs or musical instrument courses
- culture or youth centers
- immigration centers
- social clubs or neighborhood centers
- businesses
- private dormitories or student houses
- outside activities and gatherings, such as concerts, social gatherings, or picnics.

Knowledge of the existence and locations of hotspots is essential for the prevention of recruitment because frequently recruitment connections are made through the various activities that are conducted in these places, and where social networks are created. Hotspots are used to facilitate the first three steps of the recruitment cycle because they do not overtly represent terrorist organizations, and they operate legally.
**Significant Dates and Events**

Terrorist organizations observe special days, occasions, or times for celebrations or grieving. These times of remembrance are exploited to mobilize their supporters and base, to spread propaganda, and to attract people to their events. While not all special dates are directly associated with terrorist organizations, they nevertheless try to dominate these occasions to further their objectives.

For example, May 1\textsuperscript{st}, International Workers’ Day, has always been an important calendar event for leftist and Marxist terrorist organizations. It is a day when they do their best to increase the numbers of members and supporters to carry out demonstrations during events and celebrations on this day. Similarly, Hezbollah supporters come together in masses to celebrate Ashura Day. These events usually serve to provide a show of strength and an opportunity to invite non-affiliated people to the celebrations and share food and establish connections.

It is essential for individuals and teams to be aware of these dates and find out what types of activities different terrorist organization members and supporters engage in, so that they are not caught off guard when these occasions occur. In addition, these events and gatherings are significant opportunities for the prevention teams because they can easily spot newcomers and interact with them afterward.

**Who is Targeted for Recruitment?**

It is true that most terrorist organizations constantly try to recruit new members to their ranks. However, there is always a dilemma when it comes to recruitment: “security.” Terrorist organizations by their very nature have to operate secretly. The unarmed wings of terrorist organizations function under lighter rules of secrecy, as opposed to the armed cells. Therefore, when it comes to face-to-face recruitment, terrorists cannot carry out their activities openly, recklessly, and without consulting their peers and leaders. This is so in order to protect both the group and its members from law enforcement, intelligence operations, and infiltration. Terrorist recruitment is not like open hiring. Recruiters cannot reveal and declare their intentions, and they certainly cannot advertise, unless it is done through anonymous social media calls, such as those posted by ISIS. This is why there is a calculated recruitment process and cycle – it serves to ensure the secrecy and safety of the recruiters.

Prevention teams must have a good understanding of which terrorist organizations target which segment of the population, whether an organization engages in opportunistic recruitment or goes after specific individuals by talent spotting, and what the general schemes and tactics of recruitment teams and individuals consist of. The following section analyses the most commonly targeted groups when it comes to terrorist recruitment.

**Family Members and Close Friends**

Terrorists tend to recruit people whom they already know and trust, including family members and close friends. This is done so that the nature of their activities remains veiled and protected and reduces the risk of a complaint being filed to the authorities. The recruitment of family members and close friends is usually the first choice of recruiters, for three reasons.

The first reason is that terrorist recruiters have already known their family members and close friends for years. With their characteristics and qualifications, particularly those of their siblings or nieces, nephews, or other relatives close to themselves in terms of age and of close friends from their neighborhoods or schools, they are given a head start in the recruitment process, since they do not need to spend time on the initial contact phase after getting the approval for “identification of the candidate.” For example, “The IRA recruited, most commonly, trusted families whose affiliation went back generations: most operatives’ parents
and even grandparents had been involved with the movement.” Furthermore, in most cases, relationships and connections with family members and close friends generally would not raise suspicion if intelligence and law enforcement agencies are conducting investigations, since communications between friends and family members can easily be deemed non-suspicious. From this perspective, the Brussels and Paris attacks of 2016, for which close family members and friends were quickly enlisted, were, unsurprisingly, able to stay under the radar of local intelligence and law enforcement agencies in at least two countries, France and Belgium.

Second, most family members and close friends would be familiar and perhaps recognizable believers in the ideology of a particular terrorist organization and already socially related to people who believe in similar ideologies and causes. At the least, they might be believers in an ideology without embracing its violent part, like assuming a Salafi/Wahhabi lifestyle, or they might already be acquainted with the justifications used by a terrorist organization, such as the Israel-Palestinian conflict that Al-Qaeda often raises. Nesser describes this as “the existence of a ‘culture for recruitment’; implying horizontal patterns of recruitment, in which hard-core, mainly politically driven, jihadist activists with ties to known groups, quite aggressively reach out to potential recruits through their social networks.”

The third reason is the confidentiality and secrecy developed through the past connections and the advantages of being able to trust close friends and family members not to expose recruiters by tipping off law enforcement agencies and being able to easily weed out potential informants. Kenney, from this perspective, points out that “recruitment might require selecting ‘people of confidence’ — individuals who might be related to existing members to weed out potential informers or police plants.” One of the essential steps of opening up to a prospective recruit is talking about the terrorist organization. While this stage does not take place until the middle of the recruiting process, there is always a risk that it will backfire, revealing the objective and identity of a recruiter, and at worst, leading to a complaint being filed with the authorities. Due to emotional attachments and blood connections, family members and friends can generally be depended on not to turn to the authorities if they do not want to be part of the process, and they will simply look the other way; this places them among the best candidates for recruitment.

According to data I gathered in 2001 from various terrorist organization members, introduction to a terrorist organization took place with the help of friends 35 percent of the time and through family members 26.5 percent of the time. A similar pattern held for ISIS when it came to reaching out to associates or establishing new contacts in the West. According to research on ISIS cases in the US by the George Washington University Program on Extremism (GW Extremism Tracker, 2018), while digital media are one means of connection, terrorist recruiters prefer, wherever possible, face-to-face interactions.

The importance of the family bond was, for instance, revealed when the ISIS Paris and Brussels attacks cell was examined: two pairs of brothers from two different families were involved in the attacks - brothers Salah Abdeslam and Brahim Abdeslam and brothers Ibrahim el-Bakraoui and Khalid el-Bakraoui - with some of other cell members being close friends.

One also could find a similar pattern in July 2017, when ISIS planned to blow up a commercial passenger plane flying out of Sydney. The Khayat brothers, Khaled Khayat and Mahmoud Khayat, in Australia, were contacted by their elder brother, an ISIS commander in Syria, to carry out the plot. Even though the Khayat brothers had no prior connections with ISIS and were living seemingly ordinary family lives and running businesses, their older brother was able to convince them to carry out the planned attack, an attack which they attempted but failed to conclude.

Another example comes from Indonesia, where a girl was able to convince her entire family to carry out the hijra (emigration) to move to Syria to join ISIS:

“When Indonesian schoolgirl Nur Dhania arrived in Syria in 2015, she knew
almost immediately that convincing her family to join her in the ‘caliphate’ was a catastrophic error. Just 15 years old at the time, Nur Dhania said life under Islamic State rule was nothing like the paradise portrayed in the group’s propaganda. Nevertheless, 25 of her relatives - including her grandmother, sisters, parents, uncles, aunts and cousins - followed her.70

Finally, recruitment prevention teams and members must understand the importance of how terrorists usually attempt to recruit first from their own close circles for the reasons discussed above, before trying to reach out to others with whom they do not have prior and natural connections. While this puts recruiters’ families and friends into a vulnerable position, it also provides insight into opportunities for early intervention in terrorist recruitment.

University and High School Students

Historically, universities and high schools have been fertile grounds for political and ideological movements and have been infiltrated by terrorist organizations, based on their locations and the opportunities they afford. This enables terrorist organizations to operate clandestinely in schools.

Many young people are vulnerable and more at-risk for joining terrorist groups for a variety of reasons. Students sometimes establish close friendships with terrorist recruiters during and after class hours. The strong emotions and enthusiasm of some young people can drive them to make unwise choices; in addition, group thinking often preempts critical reasoning, so that some students may find themselves doing things with their group they would not consider doing alone.

Many locally operating terrorist groups establish committees or appoint a member to organize the recruitment activities in high schools and universities. Recruiters try to find ways to spend time with students through a variety of activities, such as games, sports, and joint studying, so that they can eventually create a strong enough bond to be able to start recruiting.

In 2012, a 15-year-old female high school student in Sanliurfa, Turkey, was able to recruit over 50 students from her school in the course of one year, simply by befriending them and persuading them to join the terrorist organization she was representing. During my tenure as police chief, I constantly observed different terrorist organizations using schools and universities as hubs for their recruitment activities. For example, the university recruiters liked to reach out to incoming students who were not native to an area and assist them by providing lodging, meals, or other forms of support, to win their hearts and establish connections before the newcomers realized with whom they were interacting. An ISIS fighter, a student from the University of Westminster in the UK, captured and held in prison in Syria, told the BBC that “he was one of at least seven students and ex-students from the University of Westminster to join ISIS.”71

The Al-Qaeda training manual also focuses on the importance of high schools and universities for recruitment purposes. The manual refers to the university as “a place of isolation for a period of four, five, or six years … [which] is full of youths (full of zeal, vigor, and anti-government sentiments).”72 According to al-Qaeda, high school students are also among those who should be recruited. The manual refers to students above 15 years old as follows;

“I mean you have to cultivate the idea of jihad inside of them. If you ask me, "What can this young student do?" I will reply to you, "They can do the same thing as Muadh and Mu’awadh did." This is because today they are young, but tomorrow they will be adults, so if you don’t give them da’wa "making an
someone else will (but it will be for materialistic goals). However, don’t be in a hurry, because haste in this matter might destroy the da’wa.

The merits of this sector:

1. Often they have pure minds.
2. It is very safe to deal with them because they are not likely to be spies, especially after they pass the stage of individual da’wa.”

Co-Workers

Co-workers are also ideal candidates for terrorist recruitment because people spend a lot of time with each other at work, and over time, friendships and bonds between colleagues may form or even increase, resulting in suitable conditions for terrorist recruitment. Some terrorist organizations put members in charge of different working populations, such as civil servants, office workers, doctors, teachers, nurses, and laborers, or appoint more specific subunit representatives for purposes of propaganda, recruitment, and logistical support. We have also seen examples of workplace recruitment stemming from the establishment of close kinship among workers, as happened with the 2016 Brussels attack carried out by ISIS.

Prisons

Prisons play a triple role in terrorist recruitment. The first is that of a place where terrorist inmates can carry out indoctrination, propaganda, and recruitment activities. In fact, prisons act as “academies” for terrorist organizations. Historically, some terrorist groups, like the DHKP/C and other leftist groups, wanted their members to be imprisoned, so that they could be better trained on the inside and become further radicalized while serving time. If terrorists are housed together in groups, they can assign leaders and regulate the daily lives of fellow inmates. Furthermore, because they act together, they are usually able to overpower other groups or individuals, forcing them to align themselves with their group, which yields more recruitment opportunities. Therefore, there is almost always indoctrination and recruitment going on inside prisons as terrorists try to win the hearts of other inmates, particularly those who are about to be released, not only by befriending them and persuading them to join their organization, but also by providing them and their family members with perks, such as jobs, housing, education grants, and salaries, as pathways to recruitment.

For example;

“Omar Khyam, convicted of planning terrorist attacks in the United Kingdom, described how Rachid Ramda, who was later convicted of organizing the 1995 Paris metro bombings, proactively approached and befriended other inmates said: the first thing that struck me most about Rachid was the way he greeted me…. He made me feel as if I had known him for years, such a warm personality and character, making everyone feel wanted and important as if you are his best friend.”

Similarly, Benjamin Herman, a 36-year-old drug dealer and a thief in Belgium, was radicalized and recruited in prison, killing two policewomen and one bystander while he was let out on a temporary two-day pass in 2018. These types of risks have now increased with the imprisonment of returning ISIS fighters, who have access to other inmates inside prisons. In fact, Abu Musab al-Zarqawi, Al-Qaeda’s leader in Iraq, which evolved into ISIS, was arrested
for sexual assault and drug-related charges in Jordan and was sent to prison, where he was initially radicalized and received his first jihadist ideological training.\textsuperscript{77}

A second role played by prisons in recruitment is the status elevation of former terrorist inmates due to their prison time and to the fact that they have had ample time to read and study ideological and tactical materials, increasing their commitment and dedication. I personally observed how newly released inmates would quickly be assigned to leadership positions because they had become tougher and more radicalized. Terrorist organizations also closely monitor the devotion and mental states of their imprisoned members. An ISIS prisoner named Abu Abdulhaqq al-Iraqi told Heller in an interview how he was promoted to emir as soon as he was released: “I was an inmate in the Iraqi prisons. When I got out, I assumed a position…. As soon as I got out of prison, I was an emir.”\textsuperscript{78}

A third role played by prisons in recruitment stems from the fact that terrorist organizations can identify sources among the inmates, use them for information, and encourage them to reach out to their trusted family members and friends and introduce these to terrorist recruiters on the outside. I have seen hundreds of relatives and friends of imprisoned terrorists being very quickly recruited into terrorist organizations because of their former ties and emotional bonds with their incarcerated loved ones. Terrorist inmates would arrange prison visits and encourage their visitors to meet with recruiters, most of whom were put in place before the visits. In this way, terrorist organizations can accelerate the recruitment process and overcome some security and confidentiality problems as well.

\textit{Propaganda, Outreach, and Social Media}

The emergence of the internet, social media, and encrypted peer-to-peer mobile phone and computer applications became a dream come true for terrorist organizations; it enabled them to reach out to people whom, under normal circumstances, they would never have been able to reach and radicalize, sharing with them their propaganda and literature. ISIS, in particular, was a pioneer in employing social media and other digital applications to facilitate its outreach activities, by assigning some of its members to dedicate themselves solely to attracting thousands of people from around the world and eventually succeeding in recruiting some of them.\textsuperscript{79}

It is crucial to acknowledge the opportunities the internet and other technological advancements provide to terrorists, and it is imperative to understand that often these social media influencers are the initial facilitators for connections with prospects and that through such media, the vetting and recruitment process can start.

As much success as ISIS has achieved in its outreach, particularly with its Western contacts, newcomers are not automatically accepted for fear of intelligence operations and infiltration, and arriving recruits in Syria were interrogated about their connections in their countries of origin or with members within the caliphate.\textsuperscript{80}

Another consequence of internet-based mass outreach has been the increase of “lone actors,” - individuals who become self-radicalized through terrorist propaganda. In the case of true lone actors, groups might not even be aware of their existence; these self-appointed “lone wolves” simply carry out their activities without direct supervision of, or control by, the terrorist organization. This presents a further challenge for the prevention of terrorist recruitment.

\textbf{Methods of Preventing Recruitment to Terrorism}

There is no single or unified method for preventing recruitment to terrorism. Rather, a holistic approach involving a combination of the methods described below should be utilized in
comprehensive counterterrorism and prevention campaigns, based on the prospective recruits and the location, and on the terrorist organization’s ideology, activities, social base, and capacities.

Ideally, the prevention of recruitment activities should be initiated as soon as a candidate is identified by terrorists in the early stages of the recruitment cycle. This should preferably occur before a bond between the parties has been established and before the subject has started to become ideologically indoctrinated. While prevention can take place at any stage of the recruitment cycle, the more deeply a subject is pulled into the cycle of recruitment and isolated by recruiters, the more difficult it becomes to interrupt the process.

All of the tactics and methods listed in this chapter are included under the assumption that they would be legitimate and would be applied in keeping with the legal codes of the country concerned, as well as with international legal and ethical standards, particularly in respect to protecting the identities of targeted subjects and their families.

The strategies and policies listed in this section should be carried out by civil society organizations and government authorities in a collaborative way. There is no single one-size-fits-all approach, and policies regarding tactics and stakeholders should be decided upon and fine-tuned locally. In most cases, prospective recruits or their families might consider the intervention to be less than persuasive if no government representative is involved who assure them that the intervention process is backed and supported by the authorities. Also, government actors can answer questions and discuss concerns involving judicial processes and the future of their loved ones. However, in some cases, the presence of a government representative can backfire, and subjects might perceive the intervention and prevention activities as part of a counterterrorism or intelligence operation.

Therefore, prevention teams should identify the stakeholders based on the considerations listed above, along with the demographics, characteristics, and ideologies of the groups and individuals involved.

Finally, among all the tactics listed here, I would argue that the preferred one is helping families to intervene in the recruitment process to foil the terrorist recruiters and see that their loved ones are not recruited and turned into criminals.

Prevention of Terrorist Attacks

The appropriate authorities must carry out intelligence and preventive counterterrorism operations, implement measures to halt the formation of terrorist cells determined to carry out attacks or other terrorist activities, and closely monitor the actions of terrorist organizations. Preventing attacks is vital to undermining terrorist propaganda and keeping the organizations out of the news cycle, and thereby limiting their outreach and publicity.

Terrorist organizations always closely monitor government forces and look for new tactics, so they can continue to be successful in their attacks. To prevent attacks, a combination of the following elements is needed:

- Fresh and continual intelligence on terrorist organizations’ activities, not only local, but also regional and global, shared in a timely manner with appropriate parties.
- A conversance with terrorist literature, including books, journals, pamphlets, video and audio productions, and social media posts, because through these, terrorist organizations may reveal clues about their intentions or plans.
- Detailed knowledge from local authorities on the social base and its relationship with the terrorist organization. This is indispensable, because often locals can be utilized by terrorists for logistical support, such as to provide safe havens, transportation, or financial support.
● Comprehensive coverage of the local jurisdiction. It is vital that authorities know the characteristics of the areas in which terrorist organizations operate, including physical boundaries, roads, local language dialects, and hot spots utilized as fronts.
● Knowledge of past activities of the terrorist organization in the area in question, along with any other data available to law enforcement and intelligence agencies is vital.
● Experience in countering terrorism and preventing terrorist attacks, as it takes years to gain a thorough knowledge of different terrorist organizations, learning how they operate, what types of tactics they apply, and what their structures are – which are all crucial to countering terrorism activities.

Control of the Terrorist Use of the Internet

Since the use of the internet by terrorists is a subject of study in its own right (see chapter 12 of this Handbook), I will here only briefly address the importance of denying terrorists the use of these technologies to further their goals. Terrorist organizations use the internet, social media, and peer-to-peer platforms extensively for a variety of purposes, including to:

● reach out to potential recruits and new members
● distribute propaganda and other materials, including videos, journals, memes, or pdf books,
● represent the organization and to feed their followers with news of recent developments, presented from their perspective,
● communicate,
● run front operations over the Internet,
● engage in financial and logistical support activities, and
● gather intelligence.

The purpose of this chapter is not to discuss how to counter the use of the internet by terrorists. However, it is essential to carry out local, regional, and globally coordinated activities so that terrorists cannot utilize digital media for their activities, which include identifying potential recruits. ISIS’ activities are a good example of how social media platforms, including Twitter, Facebook, YouTube, and others, along with communication applications such as Telegram and dozens of other platforms, can offer terrorist organizations a multitude of opportunities to extend their outreach through the skillful use of new media. Therefore, limiting the use of social media platforms and peer-to-peer communication applications by terrorists can help authorities fight back against terrorist recruitment, both in the long and short run.

Intervention in the Recruitment Cycle and Involving the Families of Subjects

Terrorist prevention programs, including CVE and PVE initiatives, usually focus on countering the ideologies held by groups and individuals and by engaging communities and building bridges among stakeholders. The United Nations defines such actions as activities that deter disaffected individuals from crossing the line and becoming terrorists. However, these terms and concepts are highly debatable, and some scholars argue that CVE and PVE programs have evolved into “a catch-all category that lacks precision and focus.” Preventing and Countering Violent Extremism (P/CVE) programs vary dramatically throughout the world, and the terms preventing and countering are often used interchangeably, “making it difficult to discern any conceptual distinction in their application.” Furthermore, many P/CVE programs fail to
define the specifics of their goals and what they are essentially preventing without specifying the parameters for establishing short and long term successes. The intervention concept prescribed in this chapter to prevent recruitment can be considered a part of overall P/CVE efforts. However, I do not believe in the effectiveness of these programs if they are not designed to reach out to individuals personally to raise awareness and persuade them to cut their ties with the terrorist organization recruiters who are in touch with them. Therefore, I suggest considering “intervention and prevention of terrorist recruitment” as an integral concept and program, because it is designed to deal with vulnerable individuals personally and directly as soon as they are identified as potential recruitment targets by terrorist organizations, rather than functioning as a general mass outreach effort.

Understanding the terrorist culture of indoctrination and recruitment is essential for the interruption of recruitment efforts. Terrorist organizations make sure that their members learn and understand two essential rules from the beginning of their recruitment. The first rule is to “hear and obey” regardless of any circumstances, referring to the necessity of adhering to the rules of the organizations and leaders. This rule ensures that for terrorist organizations and their leaders, regardless of their position in the hierarchy, orders will be carried out without any discussion, unconditionally, both as an ideological requirement or religious duty and as an organizational rule. For example, both Al-Qaeda and ISIS, during their ideological indoctrination and military training courses, teach their cadres “hear and obey” as a rule of the organization and as part of their religious duty to obey the emirs. Followers who underestimate this rule and fail to obey are harshly disciplined. ISIS and Al-Qaeda are known for brutally punishing, or even murdering, those who fail to obey given orders. Similarly, the DHKP/C had a disciplinary committee to investigate and punish those who refused to follow orders, often ending up assassinating their own members as punishment. Therefore, this rule is designed to ensure that even new recruits will follow the rules.

This entrenched logic and the fear of reprisals makes it almost impossible to intervene if a person is fully radicalized and recruited. Terrorist organizations usually apply a variety of precautions to secure the retention of their members and to prevent defections and ideological confusion. The second rule terrorists utilize is to not involve themselves with the teachings, literature, or social media of other ideological traditions and groups, and to not communicate or discuss competing ideologies with others, not even with family members. This rule is particularly true for new members. This ensures that terrorists, particularly new recruits, are isolated from the outside world. This is seen in cults as well, as a means of reducing the risk of defection through ideological confusion, or often, through doubts about the violent tactics of an organization. The Al-Qaeda recruitment manual prescribes a similar process of mental and physical isolation in an effort to protect its new recruits.

Finally, these rules and the mindset that follows from them, pose a high barrier to the authorities or intervention teams seeking to counter terrorist recruitment. Due to the conditions detailed above, obedience to the rules and mental and physical isolation, it is extremely difficult to reach out to individuals who are radicalized or who have been recently recruited to a terrorist organization without personally connecting with them, because their communication channels to the outside world are shut down. Often, these individuals see such efforts as the counteractivities of their enemies; therefore, they are on the defensive, programmed not to listen to what the enemy is trying to feed them. This makes the work of P/CVE programs very difficult. Additionally, P/CVE programs might be counterproductive because they may target the ideologies of terrorist organizations. When a conversation evolves into the questioning of one’s belief system without an established bond and trust, there is an increased possibility that the person subject to the P/CVE efforts will automatically shut down communication and cut off mental interactions due to distrust.
Intervention in Terrorist Recruitment

I propose an intervention and prevention program aimed at intervening at the very early stages of the recruitment process, when terrorists are attempting to identify a prospect and establish contact. These would be the first two stages of the terrorist recruitment and radicalization process, which have been explained above. However, even if a subject is not successfully identified as at-risk and vulnerable during these two stages, it is never too late to intervene until the subject is fully recruited through the remaining steps.

Intervention and prevention programs must be carefully designed, and stakeholders must work with the appropriate authorities and communities, so they can locate individuals, particularly vulnerable youth, who are being targeted for recruitment. The intervention should be carried out based on the subjects, their psychology, and the conditions surrounding them, particularly in relation to their families. It is advised that direct interactions with the subjects be carefully prepared, and whenever possible, family members should be involved from the beginning of the process, for the reasons presented above.

Families and Close Friends

The next step after the identification of at-risk individuals is the initiation of the intervention and prevention process. An important consideration is that approaching an individual in touch with a terrorist organization, knowingly or unknowingly, could easily become a setback, further radicalizing that person by pushing him or her into the arms of the recruiters. Therefore, it is substantially more productive if people, including family members and close friends who are close to the individual at-risk, can be mobilized to get involved with the authorities and intervention teams. From this perspective, Koehler and Ehrt argue that “in this sense families, friends and colleagues are our ‘first line of defense’ against violent radicalization, without implying the use of these emotional relationships for intelligence gathering or policing.”

Additionally, individuals subject to terrorist recruitment activities can be very emotionally engaged due to the bonds and friendships already established with their recruiters, and it can be challenging to counter these emotions.

I also realized during my past interactions with people targeted by terrorist recruiters, particularly young people, that without the assistance, guidance, and supervision of parents or family members, including older siblings, interventions would have limited success. In my experience, halting the recruitment process of young subjects proved to be more challenging if the families were not involved. Consequently, families and friends are the best protectors of their loved ones. They can usually keep a constant eye on their children and friends, and they are certainly a lot better at supervision than outsiders or intervention teams. Also, the involvement of the families is also beneficial in regard to protecting the siblings and close relatives of the prospects, who also often become the targets of recruiters.

How to Identify Potential Recruitment Subjects

Because this model is based on interrupting the recruitment process in as timely a way as possible, it is essential to identify potential candidates as early as possible. There are a number of ways to do this that involve different stakeholders, including law enforcement agencies, counterterrorism authorities, local partners, school administrators, and social media interactions.

First, the most reliable way to identify potential targets is through continual law enforcement and counterterrorism work. Based on how they are set up, law enforcement agencies and counterterrorism authorities carry out counterterrorism investigations daily, just as the FBI does in the US. These agencies are the best sources for determining if a known
terrorist recruiter is approaching a potential subject. Counterterrorism identification of the subjects can be done easily through investigations of cases or individuals, and by uncovering terrorists’ connections through intelligence work or forensic examinations of evidence, such as data from electronic devices, cell phones, computers, email accounts, peer-to-peer communication applications, and so forth.

In this case, the counterterrorism authorities must decide how to best reveal the identity of such a subject and/or approach that individual, based on the particular circumstances of an operation. In my case, when I administered a counterterrorism program in Sanliurfa, Turkey, I tried my best to extract as many names as possible for intervention purposes, even in some cases risking an ongoing operation, so we could interrupt the recruitment of an individual.

Stand-alone intelligence operations targeting terrorist organizations through electronic surveillance activities disclose almost all possible new recruits, because during the identification and initial contact process, even if the recruiters are careful with their communications, whether via cell phones, emails, applications or social media, their subjects are generally not so careful, at least up to a certain point. Usually, depending on the circumstances, intelligence agencies can easily share appropriate names with the intervention or prevention authorities without compromising their operations.

The analysis of open source social media like Twitter, Facebook, and peer-to-peer applications can reveal a lot of names of people who are interacting through known terrorist channels, and even ascertain their locations.

Counterterrorism authorities should monitor people, particularly students, and interact with known terrorist-affiliated fronts, including their foundations, associations, neighborhood study centres, bookstores, and any other sites the organizations employ to recruit. Additionally, events sponsored by terrorist organization fronts, such as concerts, demonstrations, meetings, training courses, and sports activities, serve as occasions for identifying candidates. Families whose children have already been recruited to a terrorist organization and who are being sought through outstanding warrants, or have become foreign fighters by moving to a conflict zone, are under the constant threat of further efforts to have other family members recruited. Therefore, special consideration should be given to the siblings of recruits among the groups mentioned above, even if they do not interact with known terrorist recruiters.

Furthermore, the family members, siblings, cousins, and nephews of imprisoned terrorists, and those who have conflicts with government authorities, should also be considered vulnerable. These family members are under constant threat of recruitment, as terrorist organizations often use their connections and emotional leverage to recruit among family members via special handwritten notes from prison or specific requests via intermediaries like lawyers or other family members who have access to prisons. These people also should be considered high-risk and vulnerable.

The groups listed above are not criminals or terrorists, nor should they be considered such. They certainly should not be profiled in terms of their affiliations; rather, they constitute vulnerable groups terrorist organizations tend to recruit more easily than outsiders. Therefore, reaching out to individuals among these targeted populations could easily help authorities prevent the recruitment of new members if they can intervene in a timely and professional manner.

**The Logic and Method of Intervention to Prevent Recruitment**

The foremost critical aspect of preventing terrorist recruitment is intervention. The goals of the authorities and teams intervening should be clearly defined and specified, and they should be openly communicated to those on-site - in this case, mostly the parents and other family members. The initial communication with the families is critical. Conveying the objectives is one of the toughest hurdles in this process because often family members may believe their
loved ones are about to run away any moment to join a terrorist organization or are in danger of being arrested. Therefore, the concept of the program and the message that the objective of the intervention program is to prevent recruitment so that their loved ones do not become terrorists should be clearly communicated as soon as the initial interactions start.

The second most important procedure is not to stigmatize families by appearing in their neighborhood as counterterrorism officers, law enforcement agents, or representatives of a government agency, in an effort to make families comfortable to meet with the authorities.

Third, clear messages that the intervention team is not conducting a counterterrorism or intelligence operation and that their loved ones are not under the threat of arrest through their family interactions should be conveyed, so that the family members can be relieved from the stress of those outcomes at the beginning of the interactions. The message that “we are here to help you help your children or loved ones, so we can save them from the hands of terrorist organizations together”, coming from the intervening authorities, is essential at this step.

The ideologies of the family members or their loved ones should never be an issue during these interactions. The prevention of terrorist recruitment is not a deradicalization program. Discussions of ideological or religious beliefs are often counterproductive and, in this case, are not among the objectives for the prevention of recruitment. Authorities should always respect the ideologies and belief systems of the families. Instead, the message that “people are free to believe what they would like to believe, as long as their activities do not involve violence” should be conveyed if ideological issues emerge.

At this intervention stage, when the authorities, teams, and individuals meet with the families, the following messages should be communicated for a successful prevention program:

- The teams are not here to investigate. This is a prevention program, and there are no judicial or law enforcement investigations involving their loved ones.
- There has not been, and will not be, any official recordkeeping; these activities are not going to show up in any records going forward.
- There is no ongoing judicial process involving the subject, and the teams are here to prevent such a process by making sure that the subjects do not become members of a terrorist organization.
- The team is not here to collect any information or intelligence, and they are not going to make any requests or try to acquire any information regarding the terrorist organizations trying to recruit the subjects. (Such a message is essential to ensure family members that their loved ones are not going to become informants, and that the objective of the visit is not to make progress in that direction).
- This prevention process is voluntary and is not a legal requirement; rather, the team is here to help the subject through the involvement of the family.
- The team members would like to work with your family so they can assist you in helping your children from being recruited. (The team members should not meet with the subjects unless the family members request it, and the initial interactions should not involve the subjects if the families are deemed to be cooperative.)
- Interactions and observations will continue until the teams make sure that the subjects cut their ties with their recruiters. The teams will be in touch with the family in the case of possible risks or unforeseen developments involving their loved ones, such as attempts to run away or ongoing relationships with terrorist groups.
Example of a Recruitment Prevention Program: Sanliurfa Program for the Prevention of Terrorist Recruitment Through Early Intervention by Involving Families

I designed an intervention and prevention program specifically to establish initial contacts with the families of vulnerable youth in Sanliurfa, Turkey; it was implemented between 2010 and 2014. The program was meant to interrupt the recruitment process of terrorist organizations in Sanliurfa, where I was police chief for counterterrorism. Our team members consisted of male and female police officers who had degrees in social work and psychology. They spoke Arabic and Kurdish, as well as Turkish, so they could communicate clearly with the families of the subjects.

Our prevention process started as soon as we identified possible subjects of terrorist recruitment. First, we opened positive communication channels with the families to build mutual trust. We made sure that they understood that we were offering assistance to help them save their children from being recruited by terrorist organizations. When we met with them, we also promised both the families and the subjects that they were not going to face prosecution or investigation if they cut their ties with the terrorist organizations. Our ultimate objective, which was clearly communicated to the families, was to persuade the prospective recruits to cut their ties with their recruiters, distance themselves from terrorist organizations, and accept professional and psychological assistance, if necessary, with the participation of their families. We also wanted to make sure that the families would be part of the prevention and recovery process.

This program became very influential as it progressed. At first, some families were reluctant to accept our help, and there were lack of trust issues. However, as people realized that we were sincere in our efforts and recognized that dozens of children were saved from joining terrorist organizations, some families started to reach out to us on their own. The success rate of the program during the first four years was 87 percent, meaning that our efforts prevented around 2,000 people from being recruited by terrorist organizations between 2010 and 2014. One of the most important findings from the program was the fact that 88 percent of the families indicated that they had not been aware of their loved ones’ interactions with terrorist recruiters. This gave us a clear indication of how terrorists, even at the very early stages of the recruitment cycle, ensured that the rules of isolation and secrecy were readily applied.

Counterterrorism/Intelligence Investigations and Operations

Many counterterrorism operations, investigations, and intelligence collection activities are great opportunities to undermine and interrupt terrorist recruitment activities. Furthermore, counterterrorism operations reveal new names associated with terrorist organizations in almost every case. Terrorist organizations usually structure themselves in cells, which provides security safeguards that enable them to continue to operate, even if there are mass arrest operations that threaten their structure. However, these cells are typically found in the armed wings or the senior-level members of the group; recruiters are not usually members of terrorist cells, and they are not in hiding.

Consequently, each counterterrorism operation is a new opportunity to uncover new and unknown names of people who are associated with a terrorist group and whose connections can improve the authorities’ grasp of the organization, whether the people are subject to recruitment or part of the recruitment teams.

Furthermore, the analysis of evidence acquired during counterterrorism operations, including digital evidence such as data from computers, cell phones, hard drives, flash drives, CD-ROMs, and cameras, and handwritten notes, connections lists, and any other material which might help uncover new names or clues, is essential to investigating recruitment
operations. Not only can counterterrorism authorities build court cases based on such evidence, but each finding and new name can prompt a new investigation and contribute to the undermining of recruitment activities.

The last consideration from the counterterrorism operation perspective is the social media and internet activities of terrorist organizations at given locales. Counterterrorism authorities can track down individuals who are interacting with known terrorists through social media accounts, internet sites, and peer-to-peer communication applications. Given the fact that terrorist propaganda is now significantly present and proliferating on the internet, it is essential to trace terrorist accounts and determine if anyone is interacting or communicating through them, which can enable local authorities to intervene.

**Following Front Establishments, Recruiters, and the Base**

Counterterrorism authorities should closely monitor the social base of a terrorist organization, its public activities designed to gather people together and attract outsiders, its known active recruiters, and its front operations. Front establishments are one of the best sites for terrorist recruiters to meet people who are interested in becoming more affiliated with a terrorist organization or who are disposed toward a given terrorist ideology that attracts them to the terrorist front organizations.

Terrorist-sponsored public events can also attract thousands of people and give the organizations a considerable amount of opportunities to meet new people and extend their base. In particular, events carried out under innocent-looking religiously affiliated covers can attract many under the guise of attending an honest and sincere program, but can, in fact, be sites where terrorist affiliates have platforms and means to reach out to attendees. For example, Hezbollah has been very successful in attracting people to its Ashura Day celebrations. Similarly, Turkish Hezbollah has been successfully gathering thousands of people for its Mawlid an-Nabi ["Birth of Prophet Muhammad"] celebrations. The last such gathering I observed as the chief of counterterrorism in Sanliurfa in 2013 brought over 35,000 people together for an outdoor event.

The DHKP/C used to host concerts at sports arenas and stadiums through its music group affiliates, where the musicians and singers would openly push the propaganda of the terrorist organization. Members of the organization would distribute their newspapers, journals, and pamphlets to the attendees, most of whom would be high school and university students who happened to be there for the music and entertainment. I remember that such a concert in Ankara in 1997 attracted around 8,000 people, mostly youth, and the terrorist organization took advantage of the opportunity to connect with a large number of students. In one of the interviews with a captured terrorist, she told me how she was first recruited at this concert in 1997 and became involved with the DHKP/C members. Likewise, after-school activities, including sports activities such as football or basketball, specific courses like karate, or neighborhood study groups, are occasions where terrorist recruiters can attract young students and spend time with them for recruitment purposes.

Terrorist bases may not necessarily involve people who are carrying out illegal activities, but they can offer opportunities for terrorists to mobilize the assistance of people, based on their ideologies and belief systems. Often, people in the base might want to distance themselves from the violence and are not eager to get directly involved in terrorist operations, but the organizations can easily enlist their indirect and passive support since they might make connections through their ideologies or through family/friend relationships.

For example, I once arrested a terrorist who left eight sticks of dynamite hidden in a bathroom scale along with some of his laundry in a duffel bag at his older sister’s house, telling her that he would pick them up later. When we searched the house, we found the bathroom weight scale with the dynamite, but the sister had no idea she was hiding explosives at her
home, where she lived with her young children and husband. Similarly, in 2012, a smuggler helped a terrorist pass through the border between Turkey and Syria and smuggled him into Sanlıurfa, took him to one of his friends, and asked if the friend would allow him to stay at his farm for a few days. The terrorist, meanwhile, met with his connections and acquired a car, which he rigged with explosives he had brought from Syria to build a SVBIED (Suicide Vehicle-Borne Improvised Explosive Device), and the car was used later for a suicide attack in Sanlıurfa. When confronted, the farm owner and his family members explained that the terrorist had stayed at their farm, but the farmer had not been involved in the attack. As can be seen from this, prior connections and ideological relationships can always be utilized to further the objectives of terrorist organizations, sometimes without the knowledge of the people involved.

Additionally, front organizations are often the best places for terrorist organizations to attract people, particularly youth, based upon their interests or ideologies. As mentioned before, these places are operated legally and are open to the public. Terrorists try to pull people into them, so that they can start interacting with prospects and target them for recruitment. Often, these front establishments are places in neighborhoods where people can casually interact through a variety of activities such as courses, training programs, sports, and reading, or where people can simply spend spare time, such as in internet cafes or tea/coffee houses. Front organizations can be extremely useful for influencing young people, who do not have much to do in their spare time and who are vulnerable to radicalization and recruitment. Terrorists also target certain neighborhoods with fitting and more attractive front establishments, based on the demographics and opportunities of the jurisdiction in which they are operating.

Moreover, legally, it can be challenging to close these places, since they do not directly represent terrorist organizations, and in the courts, it might sometimes take years to prove ties to a terrorist organization - meanwhile, they can continue to operate freely. Therefore, monitoring front organizations and establishments is one of the essential tasks in preventing terrorist recruitment. Families can easily be alerted about their children’s interactions with the people in these places and informed of their real intentions. Sometimes charities are used as fronts. In 2002, the United States Department of the Treasury designated the Global Relief Foundation (GRF) an NGO based in Bridgeview, Illinois, as a terrorist entity, after the FBI raided it on December 14, 2001. The GRF began its operations in the US as a charitable nonprofit organization in 1992 with tax-exempt status and continued its activities until the end of 2001, all the while supporting Al-Qaeda and some other Salafi Jihadist terrorist organizations.

Schools and Universities

Educational Institutions can easily become breeding grounds for terrorist organizations, particularly high schools and universities. It is easy for terrorist recruiters in schools to get acquainted with their fellow students, as they spend ample time together, which makes the school setting very suitable for radicalization and recruitment. Therefore, counterterrorism authorities should closely monitor the movements and activities of terrorist organizations at schools, with special attention given to hot spots and schools where terrorists are known to have recruited successfully in the past. Authorities should also be in touch with school administrations and teachers. Moreover, when appropriate, counterterrorism agencies should give informative seminars on the tactics of terrorist recruiters, so teachers and administrators can be alerted to signs of recruitment activity and contact the authorities. Such preventive measures are vital where there is intense recruitment activity; these can serve as an early warning system with the participation of the schools.
When I was the chief of counterterrorism, for more comprehensive and successful prevention, we assigned one experienced and trained counterterrorism officer to each high school and middle school in the city of 2.5 million people. These officers had this assignment in addition to their daily duties. Each officer visited school administrators and school social workers to talk about the objectives of their assignment, describe the tactics and methods terrorists might try to use, and exchange cell phone numbers so school officials could reach them directly, if need be. We also assigned senior management officers, like captains, to the schools deemed vulnerable and critical. They monitored these schools very closely and interacted with the school administrators. To Harran University in our city, with over 20,000 students, we dedicated a team of officers led by one officer who was designated as the university counterterrorism police captain, to monitor the activities of terrorists in and around the university. However, these officers were not tasked for investigations or intelligence collection; they were simply liaison officers, and their main job at the schools was to make sure that no student was being recruited and that no known terrorist recruiters were operating there.

In addition to these counterterrorism officers, to each school, we assigned a patrol car with at least two officers to be present and visible in front of the school gates before school started and when it finished, not only to deter criminals, but also to send the message that we were taking the protection of the students seriously in regard to any type of crime, including terrorism. While such precautionary and preventive measures may not be feasible for every jurisdiction, due to limited resources, in our case, they were very effective, as the number of new terrorist recruits among the students decreased by at least 50% during the first year these measures were put in place.

Community Policing

Counterterrorism authorities cannot control every single movement of terrorist organizations in their jurisdictions. There are always going to be terrorist activities that slip through the cracks. However, police presence and community policing activities are great tools for reaching out to communities to detect possible terrorist activities. Furthermore, in many cases, through the interactions of regular law enforcement work, tips may be offered up by people who are willing to talk to officers directly about what they have observed, if they trust the police. Therefore, community policing activities and regular law enforcement work can contribute to counterterrorism activities and the prevention of recruitment by establishing strong relationships between the communities and authorities.

Furthermore, basic law enforcement work, including patrolling the streets on foot or by cruiser or interacting with people in their own neighborhoods, always provides great opportunities for law enforcement agents to monitor a community for terrorist activities, principally if they are trained on how to spot various terrorist activities. For example, some terrorist organization members may dress or act in certain ways, especially if they are not trying to hide. This was true for ISIS members, who dressed in a particular style, with long hair, beards, and shaved mustaches. While not everyone who looked like this qualified as a terrorist, these types of clues, along with other attributes, can lead to new findings. For example, in this case, one could easily distinguish ordinary Muslims who were growing their beards from ISIS members, who had long hair, as well as long beards.95

Hotlines and Helplines

A hotline can be a lifesaver, especially if the purpose of a preventive or assistance hotline is clearly communicated to the community, and the anonymity of callers is guaranteed and
respected. In practice, authorities cannot reach everyone who is being approached or identified for recruitment purposes. However, people who are aware of terrorist recruitment activities and who do not want to call 911 or contact authorities directly can easily make an anonymous call to help others. Different countries have a variety of established mechanisms to prevent terrorist activities. For example, the German Bundesamt für Verfassungsschutz (BfV), operates an anti-terrorism hotline, for such purposes. The authorities appeal to the public to support them via confidential hotlines operating via email, mail, telephone, or cellphone applications if they have knowledge of planned violence or attack plots, know any individuals involved, see terrorism being promoted, or become aware of individuals radicalizing themselves.

Depending on the circumstances, people might sometimes be more comfortable reaching out to a hotline or helpline if an NGO administers it. For example, the National Society for the Prevention of Cruelty to Children (NSPCC) was established to help people save the children from crimes, abuse, and terrorism, with the motto “every childhood is worth fighting for.” The NSPCC defines its objective as “protecting children from radicalization,” stating, “It can be hard to know what to do if you’re worried about the radicalization of a child. We’ve got advice to help.” On its website, the NSPCC provides tips for spotting signs of the radicalization of children, noting that it can be difficult. Their information highlights children who are:

- isolating themselves from family and friends
- talking as if from a scripted speech
- unwilling or unable to discuss their views
- suddenly displaying a disrespectful attitude towards others
- showing increased levels of anger
- becoming increasingly secretive, especially regarding internet use.

Every submission to these hotlines should be investigated thoroughly to make sure that the subjects are evaluated well enough before a case is closed, regardless of the hotline or caller. Khuram Butt, the ringleader of the 2017 London Bridge attack in the UK, was apparently reported to an anti-terrorist hotline but later passed a background check when applying to work for the London underground metro system.

**Tips or Designated Hotline Numbers and Investigations**

Designated hotline numbers to dispatch centers or dedicated numbers for terrorism-related tips, like the one used by the NYPD or the FBI tip line, are important tools for preventing or signaling recruitment and other terrorist activities. Law enforcement tip lines might be the fastest and most reliable resource for people who are seeking a quick solution or who see something they believe is credible enough to report. Tip lines are also essential for investigative purposes, particularly in the wake of a terrorist incident.

In the US, the FBI established such a tip line modeled after 911, which, according to the agency, receives about 100 actionable tips every day. For example, over half of the 50,000 tips submitted to the FBI within the first two days following the Boston Marathon bombing in 2013 were submitted through the website www.tips.fbi.gov.

Another important aspect of tip lines is the ability to relate seemingly regular crimes to terrorism-related incidents. These could be as simple as an arson being called into the dispatch center and the responding officers’ having been informed about the intention of a terrorist organization to carry out such an attack, so that the possibility of a connection can be considered.

Furthermore, officers who respond to regular crimes might find out possible connections to terrorism after an initial assessment. For example, in 2012, when the dispatch center in Sanliurfa, Turkey, received a call in the middle of the night about the vandalism of a hair salon, the responding officers initially reported that the suspect was drunk and under the influence of
drugs and concluded that it was a random attack. However, later, they realized that the suspect broke the salon windows because the owner had recruited his fiancée to a terrorist organization while she was working at the salon, and the terrorist organization had sent her abroad without his knowledge.

**Conclusion**

Regular law enforcement practices often assume that counterterrorism operations, like arresting terrorists, are the same as preventing terrorism, when in fact, with terrorism, this is not the case, because terrorism involves ideologies, and terrorists often dedicate themselves fanatically to their causes. This chapter on the prevention of recruitment to terrorism, as a first line of defense, examines and offers a variety of tactics and methods that can be used to decrease terrorist organization membership, which, in turn, can reduce the numbers of terrorist attacks and related causalities.

Prevention activities are always less expensive and require fewer resources than other methods of counterterrorism. Additionally, if a prevention program is developed properly and becomes successful, it might eventually lead to the extinction of a terrorist group further down the time-line, simply because these organizations cannot survive without recruiting new members. However, prevention of recruitment to terrorism is not a stand-alone counterterrorism method and should be utilized in conjunction with other counterterrorism and preventive measures. Nevertheless, it could certainly be the most effective counterterrorism method; particularly, given the fact that many of the other measures the world took to deal with Al-Qaeda after the 9/11 attacks had questionable outcomes.

Finally, when it comes to the prevention of terrorist recruitment policies, there is no one-size-fits-all approach. A combination of approaches and policies, many of which are presented in this chapter, should be applied holistically, based on demographics; population characteristics; terrorist organizations and their ideology, their social background and base – but also the psychology of the individuals involved.

For a successful intervention, it is essential that terrorism prevention teams reach out to the individuals targeted by terrorist recruiters, and, if possible, work with their families and close networks as support groups, before they become radicalized or are indoctrinated into terrorist ideologies. In addition to these ideologies, social networks, schools, neighborhoods, and various local and global pull factors are essential factors in terrorist recruitment that should be considered in any intervention program. It is also vital that policies aim to identify individuals as soon as they start to interact with terrorist recruiters, so that intervention can be initiated at the very early stages of the terrorist recruitment cycle, and certainly before an individual is recruited or gets involved in crimes. Each and every human soul deserves a second chance, as life is nothing without mistakes, especially for youth, and it might well be, as I believe, that reaching out to vulnerable prospective recruits before they are radicalized and criminalized is the best way to counter terrorism.

Dr. Ahmet S. Yayla is Assistant Professor at De Sales University’s Homeland Security Department. He is also a Research Fellow at the Program on Extremism at George Washington University and a faculty member at Georgetown University’s School of Continuing Studies. Ahmet Yayla served previously as a Full Professor and Chair of the Department of Sociology at Harran University in Turkey. He is a 20-year veteran of the Counterterrorism and Operations Department in the Turkish National Police and served as the Chief of Counterterrorism in Sanliurfa between 2010 and 2013. He is an experienced practitioner in counterterrorism and has advised senior government officials around the world during his career in law enforcement and academia. Ahmed Yayla has published both scholarly
works and written or co-authored numerous articles on mainstream news platforms related to counterterrorism and homeland security.
Endnotes


6 Bloom, Mia, ‘Constructing Expertise: Terrorist Recruitment and “Talent Spotting” in the PIRA, Al Qaeda, and ISIS,’ Studies in Conflict & Terrorism, 40(7), 2017, pp. 603-623..

7 Ibid.


10 Jensen, Michael A., Anita Atwell Seate and Patrick A. James, ‘Radicalization to Violence: A Pathway Approach to Studying Extremism,’ Terrorism and Political Violence, 2018..


15 Ibid.


23 Ibid.
29 Al Qa’idy 2010.
30 Ibid.
32 Ibid.
33 *Dabiq*, Issue 1(7–8), p. 11.
34 Al Qa’idy 2010.
35 Ibid.
36 Ibid.
37 Ibid.
38 Ibid.
39 Ibid.
42 Ibid.
43 Al Qa’idy 2010.
47 Jensen, Atwell Seate, and James 2018.
48 Ibid.
54 Bokhari et al. 2006.
57 Yayla, Ahmet S., ‘Turkish ISIS and AQ Foreign Fighters: Reconciling the Numbers and Perception of the Terrorism Threat,’ *Studies in Conflict & Terrorism*, 2019.
59 Al Qa’idy 2010.
64 Bokhari 2006.
72 Al Qa’idy 2010.
73 Ibid.
74 Brandon, James, ‘The Danger of Prison Radicalization in the West,’ *CTC Sentinel*, 2009. Available at: https://etc.usma.edu/the-danger-of-prison-radicalization-in-the-west/.
75 Lenoir, Francois and Christopher Stern, ‘‘Radicalized’ Belgian convict kills three before being shot dead,’ *Reuters*, 29 May 2018. Available at: https://www.reuters.com/article/us-belgium-shooting/gunman-kills-three-before-being-shot-dead-belgian-police-idUSKCN1IU0VS.


Heller, Sam, Twitter post, 11 October 2018. Available at: https://twitter.com/AbuJamajem/status/1050305713204023297?s=20.

Speckhard, Anne and Ahmet S. Yayla, ‘Eyewitness Accounts from Recent Defectors from Islamic State: Why They Joined, What They Saw, Why They Quit,’ Perspectives on Terrorism, 9(6), 2015.

Speckhard and Yayla 2016.


Heydemann 2014.

Speckhard and Ahmet 2015.


Ibid.

Ibid.


98 Ibid.


100 New York City Police Department (NYPD), ‘Contact Us,’ NYPD. Available at: https://www1.nyc.gov/site/nypd/about/about-nypd/contact-us.page.

101 Federal Bureau of Investigation (FBI), ‘Submit a Tip,’ FBI. Available at: https://www.fbi.gov/tips.

Bibliography


*Dabiq*, Issue 1. Available at: https://www.ieproject.org/projects/dabiq1.pdf


Federal Bureau of Investigation (FBI), ‘Submit a Tip,’ FBI. Available at: https://www.fbi.gov/tips.
Heller, Sam, Twitter post, 11 October 2018. Available at: https://twitter.com/AbuJamajem/status/1050305713204023297?s=20.
Mezzofiore, Gianluca, ‘Isis leadership: Who’s Who in ‘fluid’ Islamic State structure of power,’ International Business Times, 2015. Available at:


New York City Police Department (NYPD), ‘Contact Us,’ NYPD. Available at: https://www1.nyc.gov/site/nypd/about/about-nypd/contact-us.page.


Reuter, Christoph, ‘Secret Files Reveal the Structure of Islamic State,’ Der Spiegel, 18 April 2015. Available at: https://www.spiegel.de/international/world/islamic-state-files-show-structure-of-islamist-terror-group-a-1029274.html.


Speckhard, Anne and Ahmet S. Yayla, ‘Eyewitness Accounts from Recent Defectors from Islamic State: Why They Joined, What They Saw, Why They Quit,’ Perspectives on Terrorism, 9(6), 2015.


Swann, Steve, Daniel De Simone and Daniel Sandford, ‘At least seven from my university joined IS, says captured fighter,’ BBC News, 1 April 2019. Available at: https://www.bbc.co.uk/news/amp/uk-47772772?__twitter_impression=true.


Yayla, Ahmet S., ‘Turkish ISIS and AQ Foreign Fighters: Reconciling the Numbers and Perception of the Terrorism Threat,’ Studies in Conflict & Terrorism, 2019. DOI: 10.1080/1057610X.2019.1628613/


Web-based Resources


“Countering the Incitement and Recruitment of Foreign Terrorist Fighters: The Human Dimension.” Presented at the 2015 OSCE-wide Counter-Terrorism Expert Conference from 30 June – 1 July 2015 in Vienna. Available at: https://www.osce.org/odihr/166646?download=true


Chapter 14
Prevention of Terrorist Financing
Jessica Davis

This chapter on the prevention of the financing of terrorism will examine the international instruments and mechanisms in place to identify and prevent terrorist financing and describe and analyze the roles of the bodies involved in countering terrorist financing. It will also provide a general overview of some national-level programs, including the role of domestic financial intelligence units (and the different types generally employed.) The bodies, laws, regulations, and norms in place to prevent terrorist financing will be examined in the context of a terrorist financing framework that explores how terrorists raise, use, move, store, manage, and obscure their funds, and how (and to what extent) these bodies are able to detect such activities. Finally, a brief analysis will be offered on their role in detecting and preventing organization and operational financing, drawing the distinction between how terrorist organizations finance their activities, and how terrorist cells and individual actors finance their plots and attacks.

Keywords: counterterrorism, Egmont Group, financing of terrorism, financial intelligence units (FIUs), Financial Action Task Force (FATF), international convention, kidnapping, money laundering, ransom, United Nations, United Nations Office on Drugs and Crime (UNODC), United States.
Before the terrorist attacks of 11 September 2001, countering the financing of terrorism (CFT) was a nascent aspect of counterterrorism in the international community. The 9/11 terrorist attacks ushered in a new era of counterterrorist financing cooperation and action while building on pre-existing norms, specifically the United Nations’ (UN) International Convention for the Suppression of the Financing of Terrorism, adopted in 1999. Following those momentous terrorist attacks, the US and its allies led the international community in creating new norms and regulations, essentially demanding international action to counter the financing of terrorism. This action has primarily taken the form of the criminalization of terrorist financing at the international and national levels, the establishment of international norms to counterterrorist financing, and the provision of technical assistance to help individual jurisdictions achieve the international standard for preventing the financing of terrorism within their borders and internationally.

Shortly after the attacks, on 23 September 2001, President Bush issued Executive Order 13224, ordering the freezing of assets and blocking of transactions by individuals and entities associated with or supporting Al-Qaeda, Osama bin Laden, and other listed groups. Days later, on 28 September 2001, UN resolution 1373 (2001) was adopted by the Security Council under Chapter 7 of the UN Charter, an action that made the resolution binding on all UN member states. The resolution calls on states to prevent and suppress financing and preparation of any acts of terrorism. Other international bodies followed suit: the Financial Action Task Force (FATF), the pre-eminent norm-setting body on money laundering (established in 1989) also adopted terrorist financing as part of its mandate in October 2001. The focus of these orders, regulations, and recommendations included encouraging countries to criminalize terrorist financing, to create or expand financial intelligence units to include the investigation and prosecution of terrorist financing offences, and to create the mechanisms for freezing terrorist assets. The FATF also created international “grey” and “black” lists, essentially a designation of certain countries for their inaction on countering money laundering and terrorist financing. These efforts remain ongoing, although in more recent years, efforts to counter the financing of terrorism have also increasingly relied on public-private partnerships.

Since 9/11, a veritable industry of counter-terrorist financing bodies and activities has emerged. The international structures and programs that have been created or adapted to counter the financing of terrorism include the FATF, the Egmont Group, parts of the UN including the UN Office on Drugs and Crime (UNODC), among others. Other bodies that have a role in detecting or deterring terrorist financing include the UN Sanctions Monitoring committee, the World Bank, Interpol, the Organization for Economic Co-operation and Development (OECD) and the International Monetary Fund (IMF). Non-governmental organizations, including not-for-profit entities, have also created programs for technical assistance in countering terrorist financing. National level structures and programs to counter and prevent the financing of terrorism have also been developed and include the creation or expansion of financial intelligence units and dedicated investigative agencies or task forces.

This chapter will examine the international mechanisms in place to prevent terrorist financing and describe and analyze the roles of the international bodies involved in countering terrorist financing. This chapter will also provide a general overview of national-level programs, including the role of domestic financial intelligence units and the different types generally employed. The bodies, laws, regulations, and norms in place to prevent terrorist financing will be examined in the context of a terrorist financing framework that explores how terrorists raise, use, move, store, manage, and obscure their funds, and how (or if) counterterrorist financing actors are able to detect these activities. A brief analysis will be offered on the role of these mechanisms and institutions in detecting and preventing organizational and operational financing, drawing the distinction between how terrorist organizations finance their activities, and how terrorist cells or individual actors finance their attacks or plots. Finally, an
examination of these prevention efforts will be undertaken in the context of the prevention framework developed in chapter 2 of the present Handbook.

What is Terrorist Financing?

Before launching into a description and analysis of the technical aspects of countering terrorist financing (CTF), it is useful to articulate and describe what exactly terrorist financing is and what activities are undertaken in support of this. A conceptual framework of terrorist financing can be very useful in the analysis of counterterrorism efforts, particularly in terms of whether they are, or are likely to be, effective.

Terrorist financing has traditionally been conceptualized as how terrorists raise and move funds. However, in recent years, more expansive analysis has described terrorist financing as the ways that terrorist actors also store, manage, and obscure funds. Moving beyond just how terrorists raise and move funds is critical: terrorist actors like ISIS, Hezbollah, and Al-Qaeda have all had elaborate financing structures that have necessitated equally elaborate and professional fund management skills. Those fund management skills include how terrorists store and manage funds raised, specifically in investments to protect them from the depreciating effects of inflation and ensure that the terrorist organization is able to access funds in the future. This evolution in the conceptualization of terrorist financing is a natural response to increased awareness of terrorist financing activities, in-depth studies of terrorist financing, and a broader understanding of the different facets involved in how terrorists finance their activities beyond the simple raising and moving of money.

Beyond understanding the various mechanisms involved in terrorist financing, it is also critical to note the distinction between the various actors involved in terrorist financing. Terrorist actors (whether they are organizations, cells, or individuals) finance their activities in different ways using a variety of strategies, depending on their objectives. Terrorist organizations have very different needs for funds, and use that money in ways that differ from those of single operational cells or individuals. Organizational and operational financing generally employ the same methods and techniques for raising, using, storing, moving, managing, and obscuring funds, but differ in terms of scope and scale. As such, the differences between organizational and operational activity should also be considered in our understanding of terrorist financing and the mechanisms involved, particularly in proactive analysis that seeks to identify how terrorists might finance their activities, absent concrete intelligence.

Generally speaking, terrorists raise funds in a few main ways: through donations, criminal activities, and business models like extortion and protection rackets. Donations to terrorists come from a wide variety of sources, including:

1. from state sponsors (benefiting such diverse groups as Lashkar e-Tayyiba, Hizb-ul-Mujahideen, the Algerian National Liberation Front, and Jaish-e-Mohammed);  
2. from wealthy donors;  
3. from other terrorist groups (“terrorist patrons,” examples of which include support from Al-Qaeda to its affiliates and support from ISIS to its provinces), from support networks;  
4. from self-financing their activities through elaborate business models, involving extortion and protection rackets (as seen in Al-Shabaab), and smuggling and trafficking in drugs, goods, and people - to name a few.

Terrorists also use a wide variety of other criminal activities to raise funds, including: kidnapping for ransom, financial crimes, robbery and theft, and natural resource exploitation. Essentially, terrorists will raise funds by exploiting the economic activity in the area in which they are operating. Terrorists specifically seek to exploit any activity, licit or
Illicit, that have low barriers to entry, can generate money for their activities, and are unlikely to lead to disruption of their activities and plans by law enforcement or security services. Terrorists use money to pay for their material needs and activities, ranging from organizational needs such as food, water, logistics, and salaries to preparing terrorist attacks. The use of funds by terrorists is widespread and extremely varied, and dependent on what their objectives are. There is also a significant difference in how terrorist organizations, cells, and individuals use funds. Organizations are more likely to spend the bulk of their money on maintaining their organizational cohesion, and in some cases, maintaining territory. For instance, the Liberation Tigers of Tamil Eelam (LTTE) spent significant funds operating an entirely parallel system of governance in the north of Sri Lanka.\textsuperscript{18} For their part, cells and individuals usually spend the bulk of their funds on operational issues such as the acquisition of weapons, operational security measures (like burner cell phones and safe houses), and in some cases, bribing officials for access to sensitive sites. A salient example of how terrorists use funds for operational activities was the San Bernardino attack in 2015 in the US. The two attackers used money to construct improvised explosive devices, buy two handguns, two assault rifles, 1,700 rounds of ammunition, and to rent an SUV for use during the terrorist attack.\textsuperscript{19} Examining how, and on what items, terrorists use funds is a critical component of preventing terrorist attacks and countering the financing of terrorism. It presents opportunities to understand their intent, capability, and level of planning and preparation for attacks, as well as their longer-term plans, such as territorial control.

Terrorists also have a need to move funds as part of their financing activities. Terrorists frequently raise funds in one jurisdiction, and then need to move the money to another for use for operational activities, or for organizational support. In some cases, some jurisdictions are exploited specifically for fundraising activities, and attacks in these jurisdictions are rare. For instance, Hezbollah is widely believed to raise funds in Canada,\textsuperscript{20} but there have been no terrorist attacks by the group in that country. In many cases, funds may need to be moved from a jurisdiction primarily used for fundraising into one where a terrorist group is holding territory, or from a terrorist group to an operational cell or individual, to name but two examples of the need to move funds. Moving funds, particularly internationally, can increase the scrutiny on those funds due to the international norms and regulations set by counterterrorist financing bodies to enhance due diligence with regards to money transfers.

To move funds, terrorists use a wide variety of methods, most of which depend on the jurisdiction in which they are operating, and are dictated by the structure of the financial sector in both the sending and receiving jurisdictions. Despite the norms and regulations intended to prevent or detect the movement of terrorist funds in the formal financial sector (banks and money services businesses), the formal financial sector is still used extensively for the movement of funds, both for operations and organization support. Terrorist groups regularly use the formal sector to move funds to other terrorist groups,\textsuperscript{21} to receive funds from their state sponsors,\textsuperscript{22} when getting donations from their supporters, etc.\textsuperscript{23} Operational activity is also supported by the movement of funds through the formal sector. As Oftedal notes, the Sauerland cell (2007), the liquid bomb airliner plot (2006), the London underground bombings (2005), the Hofstad group (2004) and the Madrid cell (2004) all moved funds through legitimate financial institutions.\textsuperscript{24} Of course, terrorists also move funds in a variety of other ways, through cash couriers,\textsuperscript{25} through money services businesses and informal value transfer mechanisms\textsuperscript{26}, as well as through cryptocurrency transactions\textsuperscript{27} and trade based money laundering.\textsuperscript{28} For instance, in 2016, the Mujahideen Shura Council, active in the Gaza Strip and considered a foreign terrorist organization by the US since 2014, launched a campaign for donations. They were specific in how they wanted those donations to be given, asking for donations through bitcoin, and stating that they would use the money for the purchase of weapons.\textsuperscript{29}

To illustrate the many methods of fund movement used by terrorist organizations, the case of ISIS is instructive. The group moved money across borders through a combination of cash
couriers and informal, trust-based hawala services which are widely used in the Middle East and beyond. The methods were selected based on a number of factors, including the original state of the funds (in many cases, cash) and the ease of placing them in the formal financial sector, such as whether they had conscious or unwitting contacts in banks to help them place the funds and move them without reporting the transaction as suspicious. These decisions were based on the structure of the financial sector in the receiving jurisdiction, i.e., whether money services, businesses, hawala, or banks were more prevalent and widely used. Using multiple methods allowed the group to tailor its movement of money to the situation at hand and avoid detection, which is an important consideration for operational financing. These decisions can also be a reflection of the amount of money being transferred: in some cases, ISIS has used the formal financial sector. ISIS made use of the formal financial system to move funds to its affiliated groups, and reportedly wired $1.5 million via banks to Mindanao in the Philippines.

The variation in the funds movement mechanisms employed by ISIS demonstrates the group’s breadth and depth in terms of financial acumen, but also reflects the jurisdictional challenges and opportunities for a group with such international reach and supporters worldwide.

Terrorists must also store and manage the funds that they obtain, either for organizational or operational purposes. Terrorist groups may use one or more persons to manage their money, with some groups employing committees and sub-committee structures to oversee their funds. At the operational level, management techniques are considerably less complicated. Most terrorist cells will have one person responsible for determining how much money is needed, devising strategies to obtain those funds, and in some cases figuring out how to obtain the goods needed to conduct their attacks without attracting the attention of law enforcement or security services. For instance, in the case of the thwarted 2006 Toronto 18 plot in Canada, one individual was responsible for obtaining and managing the money for the cell. Challenges are greater for organizational management of terrorist funds, as they can generate significant wealth or resources. Compounding this, terrorist groups must also store and invest their funds to protect them from seizure, as well as from the deleterious effects of inflation. Storage of funds often takes place in cash, or in the formal financial sector. Terrorist actors also invest their funds in real estate, businesses, and even on the stock market in order to ensure that their assets do not depreciate over time. Investment of funds is particularly critical for terrorist groups that have long-term time horizons, as inflation can reduce the purchasing power of even significant sums of money. Terrorists may also invest funds outside of the jurisdiction where they are operating to protect them from counterterrorism financing measures, either kinetic (in the case of air strikes on cash storage sites, for example), or sanctions or increased jurisdictional scrutiny.

Terrorist groups, cells, and individuals use a variety of methods to obscure the source and destination of their funds in order to prevent the detection of those funds and their potential use. Terrorists work to hide management structures and where their funds are stored, which are particularly vulnerable to seizure. Financial tradecraft, which involves methods to obscure their funding, is used throughout the terrorist financing process to prevent the detection of their funds by law enforcement and other counterterrorism financing actors. This tradecraft is applied from raising funds through the movement, use, management, and storage of funds. At the same time, these are not discrete categories; many of the techniques used by terrorists have multiple purposes. Terrorists use crypto-currencies and other financial technologies to obscure their funds, as well as gaining a degree of control over a financial entity. Terrorists can use intermediaries, third parties, false identities, and nominees to hide the source and destination of their funds, as well as charitable and non-profit organizations. Some terrorist actors use money laundering techniques to obscure the origin of their funds, as well as specialists like financial facilitators. In some cases, terrorist specifically use women as nominees or even just cover names in financial transactions, as they believe that female names attract less counterterrorism financing scrutiny from banks.
In order to counter terrorist financing and prevent the financing of terrorist activity, all the methods that terrorists use to raise, use, move, store, manage, and obscure their funds must be understood, with the specific vulnerabilities outlined, and opportunities for counterterrorist financing activities illustrated. In many cases, these opportunities will be limited, as terrorists exploit territorial control for a good portion of their financing activities. In that case, the most effective counter terrorist financing activity would be to prevent or eliminate terrorist control of territory. Understanding all the mechanisms involved in terrorist financing can also help determine what, if any, international norms and regulations will be effective in particular jurisdictions to prevent or detect the financing of terrorism. Effectively countering terrorist financing requires both an organizational and operational understanding of terrorism - how terrorist organizations finance their activities - as well as the differences that exist in operational financing, and the different techniques (investigative, policy, regulatory, legislative, etc.) that are required to effectively detect and disrupt both operational and organizational terrorist financing.

**Criminalization of the Financing of Terrorism**

Efforts to prevent terrorist financing only began in earnest in the 1990s, and have led to the establishment of a plethora of counterterrorist financing bodies, regulations, norms, and institutions. These organizations are dedicated to establishing standards for countering the financing of terrorism, assessing whether states are implementing these standards and criminalizing terrorist financing, and providing technical assistance for “sub-standard” states. In effect, these organizations are responding to the international criminalization of terrorist financing.

One of the first international condemnations of terrorist financing came in 1997, the year in which the United Nations’ General Assembly (UNGA) resolution 51/210 called upon all states to take steps to “prevent and counteract, through appropriate domestic measures, the financing of terrorists and terrorist organizations....” The resolution notes that terrorist financing can occur through charitable, social, and cultural organizations, and that nations should adopt regulatory measures to prevent and counteract the movement of suspected terrorist funds, but at the same time not impede legitimate capital movements. The resolution also calls on states to share information concerning the international movement of terrorist funds. This resolution laid the foundation for the adoption of international norms to counter terrorist financing, but also to share information on terrorist financing, a key component of current prevention efforts.

Two years later, the UN adopted the “International Convention for the Suppression of the Financing of Terrorism” (Terrorist Financing Convention). While the convention was adopted in 1999, it only entered into force on 10 April 2002, following the required minimal ratification by twenty-two nations. The convention criminalizes financing acts of terrorism and also calls for the freezing and seizure of funds. This convention laid the foundation for some of the main methods of countering terrorism financing, which includes criminalizing terrorism financing, imposing sanctions, and freezing assets.

Of course, one of the main events that led to this sea change in terms of action to counterterrorist financing were the terrorist attacks of 11 September 2001 in New York and Washington, DC. Following the attacks, on 25 September, President Bush issued Executive Order 13224. The Executive Order blocks property and prohibits transactions with individuals who commit, threaten, or support terrorism, and establishes a list of individuals prohibited from transacting in the US. This list is maintained by the Office of Foreign Assets Control. This Executive Order spurred action internationally, through multilateral organizations, and domestically, amongst allies of the US, to take similar action to counter and prevent terrorist financing.
Three days later, the United Nations Security Council (UNSC) adopted resolution 1373 that requires members states to implement measures to enhance their ability to prevent and counter terrorist activities, including the financing of terrorism.\textsuperscript{43} Implementation was slow and uneven. As of 2015, while a “large number” of countries had criminalized terrorist financing, some had not yet criminalized the “financing of a terrorist organization or that of an individual terrorist, for any purpose”. The UN Counter-Terrorism Committee Executive Directorate views this as a significant shortcoming, as terrorists use funds to carry out terrorist acts, “but also to pay for preparatory acts and fund their ongoing operations.”\textsuperscript{44}

In October 2001, the FATF, a body dedicated to establishing international norms to stop money laundering, expanded its mandate to deal with the “issue of the funding of terrorist acts and terrorist organizations,” creating eight (later nine) special recommendations on terrorist financing.\textsuperscript{45} These recommendations were first published in October 2001,\textsuperscript{46} and were revised in 2012 into the current 40 recommendations, encompassing terrorist financing within them.\textsuperscript{47} The FATF recommendations are meant to provide specific guidance to states on how to implement the requirement to criminalize terrorist financing, help them establish mechanisms to prevent and detect terrorist financing, and assist in the prosecution of those offences, addressing all aspects of prevention of terrorist financing. The criminalization of terrorist financing continued beyond the immediate impact of the 9/11 attacks, with the Council of Europe adapting its Convention 141 of 1990\textsuperscript{48} to address terrorist financing in 2005.\textsuperscript{49}

According to analysis from the FATF, there are only a handful of countries that have yet to criminalize terrorist financing: Bhutan, Botswana, and Uganda. Others are partially compliant with the requirement to criminalize terrorist financing including: Bahrain, Costa Rica, Fiji, Guatemala, Hungary, Madagascar, Mauritania, Mauritius, Nicaragua, Samoa, Seychelles, Slovenia, Vanuatu, and Ukraine.\textsuperscript{50} This means that these states have taken some, but not all, steps to criminalize the aspects of terrorist financing laid out in relevant international resolutions and conventions.

The UN conventions and individual actions by member states are meant to create a wide net to criminalize terrorist financing. This has a number of preventive effects. The criminalization of terrorist financing has upstream prevention implications in that it helps to prevent the formation of a terrorist group or cell by restricting their ability to raise funds, certainly in an overt manner. It also enables law enforcement to take action on the financing of such activities, who do not have to wait until further in the process when more kinetic activities are taking place, such as bomb-making. In practice, however, many states are reluctant to proceed with terrorist financing charges in the absence of material activity. Upstream prevention is also present in the criminalization of these acts, as it helps to prevent the formation of terrorist groups or cells by restricting their funding, forcing them to spend considerable time obtaining that funding and obscuring it from law enforcement or security services. This prevention is also enabled by law enforcement’s ability to take action on the financing of these activities.

In terms of midstream prevention, the criminalization of terrorist financing helps to prevent terrorists from acquiring the capabilities to prepare terrorist campaigns, at the organizational, cell, and individual level. As the UN notes, “one of the most effective ways to combat terrorism is to prevent terrorists and terrorist entities from accessing the funds necessary for recruitment, training, and the planning and commission of terrorist acts.”\textsuperscript{51}

Downstream prevention is also enabled through this criminalization and enhanced focus on information sharing, as it allows states to use financial intelligence and analysis of terrorist financing activity to foil and deter terrorist operations. This sharing of information (specifically financial intelligence) has been significantly enhanced since 9/11, and is increasing with the prevalence of public-private partnerships, one of the most recent measures in countering the financing of terrorism.
International Counterterrorism Financing Bodies

Over the course of the almost two decades since the terrorist attacks of 11 September 2001, a wide variety of international counterterrorism financing bodies have emerged, or altered their pre-existing mandates in order to contribute to the fight against terrorist financing. Understanding how these bodies work, establish international norms and regulations, interact with each other and with states, is not a simple matter. Going further, assessing whether or not they are effective at preventing terrorist financing would involve complex analysis with many different variables, and jurisdiction-specific analysis. While not the main point of this chapter, outlining their roles and responsibilities and drawing linkages to how terrorist financing happens, can be useful in ultimately paving the way for a discussion on effectiveness, particularly as it relates to prevention of terrorist financing.

FATF is a multilateral organization established in 1989. The organization originated with a declaration from the G7 at the July 1989 meeting in Paris that established an organization to combat money laundering. In 2001, the mandate of FATF was expanded to include terrorist financing. The purpose of the FATF is to set standards for, and promote the effective implementation of, legal, regulatory and operational measures to combat money laundering and terrorist financing and other related threats to the “integrity of the international financial system” which has recently come to include counter-proliferation financing. Functionally, the FATF is a policy-making body.

The FATF has four main functions or outputs that guide the international community in the countering of terrorist financing:

1. Recommendations designed to guide countries in combating money laundering and terrorist financing;
2. Three principal typology reporting detailing trends and issues in terrorist financing;
3. Mutual evaluations of member countries’ anti-money laundering and terrorist financing regimes;
4. “Blacklist” and “greylist” of members found deficient according to FATF standards.

The FATF’s recommendations are meant to be implemented by members in order to ensure that their financial sector is able to detect and deter money laundering and terrorist financing. There are two specific recommendations that deal with terrorist financing (recommendations 5 and 6). However, references are made throughout the other recommendations to terrorists and terrorists financing, integrating the FATF’s guidance on terrorist financing into the broader recommendations. Recommendation 5 calls on states to criminalize terrorist financing on the basis of the UN’s Terrorist Financing Convention. The recommendation articulates that the criminalization of financing should extend to financing terrorist acts, as well as the financing of terrorist organizations and individual terrorists, “even in the absence of a link to a specific terrorist act or acts”, and that countries should ensure that these offences are “designated as money laundering predicate offences.” In Recommendation 6, the FATF calls on states to “implement targeted financial sanctions” in order to freeze funds and assets of persons designated by the UNSC, reinforcing calls from the UN to do the same. While Recommendation 8 is not exclusively about terrorist financing, it focuses on non-profit organizations and points out that they are subject to abuse by terrorist organizations, calling on countries to “apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organizations to protect them from terrorist financing abuse.” Ultimately, all the recommendations are meant to provide a legal framework to be implemented by states to create a robust anti-money laundering and counterterrorism financing regime.

In addition to providing the legal framework to be implemented by states, the FATF also creates reports to guide members in the implementation of the recommendations and in proactive identification of terrorist financing. The typologies are meant to inform members of
emerging risks or threats relating to terrorist financing. The FATF’s mutual evaluations determine members’ progress in implementing the recommendations, and their effectiveness in terms of counteracting terrorist financing.

The FATF’s main tool of coercion are its “blacklist” and its “greylist” - colloquial terms for formal statements issued by the organization. The FATF “blacklist” is actually the FATF Public Statement that names members who have “strategic deficiencies” in their Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) regimes that “pose a risk to the international financial system.” The FATF has called on its members and other jurisdictions to apply counter-measures to protect the international financial system from the risks these jurisdictions pose. As of February 2019, two countries were on that list: Iran and North Korea (DPRK). The FATF “greylist” is derived from the FATF statement “Improving Global AML/CFT Compliance: On-going process” and identifies countries with strategic deficiencies that are subject to an action plan. As of 22 February 2019, that list included The Bahamas, Botswana, Cambodia, Ethiopia, Ghana, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen. Presence on either of these lists can have implications for countries in terms of financial inclusion, correspondent banking relationships, and loans from the International Monetary Fund (IMF). These measures are intended to incentivize the adoption of the FATF recommendations, but the mutual evaluation process has been criticized for being politicized.

As part of the review process, the FATF has also mandated that member countries undertake a risk assessment, requiring that each country “identify, assess and understand terrorist financing risks it faces in order to mitigate them and effectively dismantle and disrupt terrorist networks.”

The FATF’s Strategy on Combating Terrorist Financing outlines a variety of activities that the organization undertakes to ensure that countries have the tools available to combat terrorist financing. The strategy seeks to:

- Improve and update the understanding of terrorist financing risks;
- Ensure that the FATF Standards provide the framework for countries to be able to identify and disrupt terrorist financing;
- Ensure countries are appropriately and effectively implementing the FATF Standards;
- Identify and take measures in relation to any countries with strategic deficiencies for terrorist financing;
- Promote more effective domestic coordination and international cooperation to combat the financing of terrorism.

The FATF’s recommendations with regards to terrorist financing are extremely broad. As such, the activities that the organization undertakes to raise awareness about current issues in terrorist financing are critical. Specifically, in 2015, the FATF published the “Emerging Terrorist Financing Risks” report, highlighting the challenges posed by lone actors and small terrorist cells, and also covering relatively new methods of fundraising for terrorist activities through the exploitation of natural resources, as well as identifying new payment products and services, and methods of fundraising through social media. While these awareness-raising efforts are critical to understanding the ways that terrorists’ financing has evolved, given that some FATF member countries have yet to criminalize terrorist financing, or have yet to implement an effective regime, these more advanced methods and techniques may fall on deaf ears in all but the most competent jurisdictions.

There are a number of FATF-style regional bodies exist that function as a global network, such as:

- Asia/Pacific Group on Money Laundering (APG), based in Sydney, Australia;
● Caribbean Financial Action Task Force (CFATF), based in Port of Spain, Trinidad and Tobago;
● Eurasian Group (EAG), based in Moscow, Russia;
● Eastern & Southern Africa Anti-Money Laundering Group (ESAAMLG), based in Dar es Salaam, Tanzania;
● Groupe d’Action contre le blanchiment d’Argent en Afrique Centrale [The Task Force on Money Laundering in Central Africa] (GABAC), based in Libreville, Gabon;
● Latin America Anti-Money Laundering Group (GAFILAT), based in Buenos Aires, Argentina;
● Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), based in Dakar, Senegal;
● Middle East and North Africa Financial Action Task Force (MENAFATF), based in Manama, Bahrain;
● Council of Europe Anti-Money Laundering Group (MONEYVAL), based in Strasbourg, France (Council of Europe).

Of course, all of these bodies have secretariats and staff associated with them, and are part of the veritable counterterrorist financing/anti-money laundering network, holding and attending conferences, workshops, and meetings.

The FATF and its regional bodies take a hybrid approach to prevention, in that some of it may be considered upstream prevention, with other activities falling into the category of midstream and downstream prevention. In terms of upstream prevention, the FATF’s recommendations and information could be conceived as working to prevent terrorist groups or cells from forming by denying them financial resources. Other work undertaken by the FATF could be considered midstream terrorism prevention, working to prevent terrorist operational activity (attacks) from being undertaken by preventing the movement of funds to operational actors. Finally, the FATF’s recommendation to criminalize terrorist financing forms part of the downstream prevention efforts advocated by the organization.

If the FATF is the strategic-level, norm and regulation-setting body, then the Egmont Group should be conceived of as its operational corollary. The Egmont Group, established in 1995, is a multilateral body of 159 financial intelligence units (FIUs) that provides a platform for the “secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing.” The Egmont Group is self-described as the “operational arm of the international AML/CFT apparatus.”

The main function of the Egmont Group is to facilitate the exchange of operational, investigative, and financial intelligence. Functionally, the Egmont Group provides access to the Egmont Secure Web, an information transfer network that ensures “security, reliability and effectiveness” for the transmission of financial intelligence. Access to the Egmont Secure Web is reserved for authorized personnel. The Egmont group members use the system to send requests for information to each other and share the results of those queries, according to what each financial intelligence unit is mandated to collect, and what their respective legislations permit them to share. This is a critical distinction because the threshold for sharing information relating to money laundering and terrorist financing via the Egmont Secure Web varies for each country. These relationships are managed on the basis of bilateral memoranda of understanding.

The Egmont Group also facilitates technical assistance such as mentoring and coaching, specialized training courses, analysis and research products, and staff exchanges. The Egmont Group also conducts research and analysis and releases reports to its members on terrorism-related topics such as enhancing information exchange between FIUs on terrorist financing issues, the “ISIL (Islamic State) Project”, information sharing challenges involving FIUs, and “Financing of Lone Actors/Small Cell Terrorism.” Phase I of the ISIL Project
“focused on developing financial profiles, indicators, and typologies” of suspected foreign terrorist fighters affiliated with ISIL, Al-Qaeda, and affiliates, while Phase II looked at foreign terrorist fighters and their facilitation networks.  

The majority of the Egmont Group’s work consists of facilitating the exchange of information relating to money laundering and terrorist financing investigations; as such their contribution to preventing terrorist financing can be largely understood as a midstream or downstream contribution effort, with their work on typologies and trends constituting their contribution to upstream efforts to counter terrorist financing.

Not all multilateral bodies dealing with terrorist financing are (inter-)governmental organizations; the private sector also has a multilateral body that has a role to play in preventing terrorist financing. The Wolfsberg Group is a conglomeration of thirteen global banks that work to develop frameworks and guidance on financial crime risks, including money laundering and terrorist financing. The group provides an industry perspective to these issues, and issues guidance and recommendations to its members. In 2002, the organization issued a statement on the suppression of terrorism financing that supported (inter-)governmental efforts to counter terrorist financing. The Wolfsberg Group’s contribution to efforts to counter and prevent terrorist financing are modest, but have laid the foundation for future public-private partnerships.

The IMF and World Bank are also part of the international counterterrorist financing regime, and work with members of the Egmont Group to provide technical assistance to developing countries, particularly those prone to “generating terrorism finance” or “with histories of money laundering.” This work is undertaken to help establish and strengthen the capabilities of their respective FIUs. As such, much of this work is meant to support the sharing of financial intelligence and the assessment of reports that may be related to terrorist financing, largely downstream prevention efforts to counterterrorist financing, as much of this information will only be shared after the movement of funds has taken place, or after the operational terrorist activity has occurred. The IMF also has a significant role in assessing countries’ compliance with international standards. The IMF conducts its own assessments of countries’ compliance as part of its Financial Sector Assessment Program and its Offshore Financial Centers Assessment Program. The World Bank’s role in combating terrorist financing has included technical assistance, as well as research, to identify areas vulnerable to financial abuse. The World Bank has also administered a database to coordinate the identification of technical assistance needs and facilitate collaboration with partners and member countries. Between 2010 and 2014, technical assistance was provided through the Topical Trust Fund.

The Role of the United Nations in Countering Terrorist Financing

The UN has a number of offices and activities that support the prevention and suppression of terrorist financing. Chief among these are the UNODC in Vienna, the United Nations Counter Terrorism Executive Directorate (CTED), and the UN sanctions monitoring teams, in New York.

The UNODC has several units involved in countering the financing of terrorism. The UNODC’s Terrorism Prevention Branch (TPB) provides training on the legal aspects of countering terrorist financing, “including promoting the ratification of the relevant universal legal instruments, in particular the International Convention for the Suppression of the Financing of Terrorism (1999), and the implementation of these international standards.” TPB works closely to deliver training and technical assistance on these issues with another unit within UNODC, the Law Enforcement, Organized Crime and Anti-Money-Laundering Unit, which is responsible for the “Global Programme against Money Laundering, Proceeds of
Crime and the Financing of Terrorism” (GPML). The GPML was established in 1997 and provides technical assistance and training on countering the financing of terrorism.66

In addition to these two bodies that provide technical assistance and training, field offices of the UNODC also undertake counterterrorism financing activities, initiatives, and training. For instance, in recent years, the Pakistan office has undertaken a workshop on countering the financing of terrorism for law enforcement agencies and private banks,87 a workshop on public-private partnership in countering the financing of terrorism,88 and training for prosecutors in countering terrorism financing.89 All these initiatives are made possible through donor funds, and are generally funded through broader projects, such as “Pakistan’s Action to Counter Terrorism” (PACT).90 At any given time, not all field offices deliver programming on counterterrorism financing; instead, it is delivered periodically and as-needed within countries.

For its part, the United Nations Security Council’s Counter Terrorism Executive Directorate (CTED also has a role in countering terrorist financing. The directorate operates under the counterterrorism committee and is composed of a body of experts. One of their main roles is to assess member state implementation of Security Council resolutions, including their implementation of UN Resolution 1373 (2001) and the establishment of FIUs.91 The UN can also impose sanctions against countries in support of a variety of security goals. These measures have ranged from economic and trade sanctions to arms embargoes, travel bans, and financial or commodity restrictions. Sanctions regimes are administered by sanctions committees, and monitoring groups are established to support the work of the sanctions committees. Some of the sanctions are implemented to deter or “constrain” terrorism. However, monitoring groups are not always established to monitor sanctions implementation.92 The United Nations Sanctions Monitoring Committee frequently deals with elements of terrorist financing, particularly in terms of information relating to the financing of terrorism (or non-state armed groups) through its investigative work. Monitoring teams have reported on the financing of terrorist activity, particularly with regards to ISIL, Al-Qaeda, Al-Shabaab, the Taliban, as well as the financing of other irregular armed groups in other conflicts, such as those in Sudan and South Sudan.93 These monitoring teams work cooperatively with the FATF and regional-style bodies.94

**Domestic Financial Intelligence Units (FIUs)**

One of the main recommendations from the FATF is for countries to establish domestic FIUs to serve as the center for the receipt and analysis of suspicious transaction reports as reported by the financial sector, as well as other information that would be relevant to money laundering and terrorism financing investigations and prosecutions. The FATF’s recommendations also include the requirement for FIUs to disseminate the results of their analysis.95 At their root, FIUs receive reports from reporting entities (defined in domestic legislation or regulations) that often include banks, but may also include money services businesses and other types of financial entities. These reports almost always include suspicious transaction reports, or an equivalent, aimed at providing a reporting mechanism for institutions to provide information on activities that they suspect may relate to money laundering or terrorist financing. In practice, the vast majority of these reports relate to fraud, financial crime, and money laundering activities, with only a very small proportion relating to terrorism and terrorist financing.

Indeed, the international regime has been plagued by the difficulties in identifying terrorist financing amongst all types of financial activities (both legitimate and illicit). In many cases, terrorist financing transactions have little that separate them from other transactions. Emphasis has been placed on the international movement of funds, but this is neither exclusive to terrorist financing, nor an activity that can help narrow down the focus to identify terrorist financing.
Fundamentally, terrorist financing and the proactive identification of terrorist financing in financial data suffers from a small data problem. Money laundering and other financial crimes are plentiful, meaning that there is significant data from which to construct rules that can be used to train algorithms for proactive detection. Conversely, true cases of terrorist financing using the official banking systems are rare, and methods of financing terrorism are often jurisdictionally specific, meaning that any indicators or rules identified in one jurisdiction do not easily translate across countries. Further, terrorist financing activity is often highly dependent on the type of terrorist entity doing the financing; as the terrorism landscape shifts quickly, these trends and typologies can quickly become outdated, making any successful “rules” implemented to sift through transactional data quickly obsolete.

To overcome this small data problem, public-private partnerships have been increasingly established between the private sector and public sector entities, specifically law enforcement and security services, and in some cases, FIUs. Indeed, some financial intelligence units, like the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), consult with the private sector, but these partnerships take the relationship further. Some have argued that partnerships between the public and private sector represent an important means to “detect, deter, disrupt and deny terrorist and other criminal organizations illicit profits and material support required to fuel their evil acts.”

These partnerships represent a blurring between public and private authority. Of course, as with any relationship between the public and private sector, concerns exist about privacy - how information (and what type of information) can be shared, and the implications for human beings (e.g. those people in conflict zones dependent on remittances from refugee family members in developed countries). Little work has been done examining these issues, making this an area ripe for scholarly research.

FIUs are often seen as the “backbone” of domestic anti-money laundering and counterterrorist financing initiatives. In fact, FIUs play a role to varying degrees in these initiatives. In some cases, FIUs play a significant and investigative role, and have broad independence in terms of analysis, investigation, and, potentially, even prosecution. In other cases, the FIUs have a very limited role and are constrained, largely acting (according to some critics) merely as a “mailbox” for suspicious transaction reports.

There are three main models for FIUs, but each country implements the recommendation to establish FIUs differently. Further, every country has varying levels of competency within these FIUs. Some are well-resourced and receive good information from their reporting entities, while others are under-resourced, poorly trained, and receive little if any useful information.

The judicial model of an FIU establishes the unit in the judicial branch of government. In this model, information from the financial sector is passed directly to an agency located in the judiciary for analysis and processing; the judiciary has authority over investigative bodies, meaning that they can direct and supervise criminal investigations. The judiciary can seize funds, freeze accounts, conduct interrogations, detain people, conduct searches, etc. Both Cyprus and Luxembourg have such judicial (or prosecutorial) FIUs.

The law enforcement model of financial intelligence units establishes the FIU as a law enforcement agency. In this model, the FIU implements the country’s AML/CFT requirements alongside the existing law enforcement system. Examples of countries with law enforcement FIUs include Austria, Germany, and the UK.

The administrative model of FIUs is very common, and involves a centralized, independent, administrative authority that receives and processes information, and then discloses it to judicial or law enforcement authorities. This type of FIU is commonly housed as part of a structure of an existing administration or agency other than law enforcement or judicial agencies, such as ministries. The FIU acts as a buffer between the financial and law enforcement communities. The role of the administrative FIU is to substantiate the suspicion
of the reporting entity prior to passing the information to investigative agencies; this allows the FIU to act as an independent validator of a given suspicion, relieving the financial institution of the burden of ensuring that it only passes on information that it is “certain” relates to a financial crime.\textsuperscript{108}

Administrative FIUs generally have limited powers, and focus on the receipt, analysis, and dissemination of suspicious transaction reports and other reports, and do not have investigative or prosecutorial powers.\textsuperscript{109} Countries with administrative FIUs include Canada, Australia, France, and Israel.\textsuperscript{110} A hybrid model of FIU also exists in which the FIU combines elements of at least two types of FIUs.\textsuperscript{111} Some combine administrative and law enforcement FIU functions, while others combine powers of, for instance, customs with police, and may be the result of combining separate agencies that had both been tasked with financial crime investigations or analysis. Countries with hybrid FIUs include Denmark, Guernsey (UK), and Norway.\textsuperscript{112}

While there are clear advantages and disadvantages to each model of FIUs, the structures and their responsibilities are often established based on domestic considerations, such as privacy laws, banking secrecy laws, etc. Comparing each model must take into consideration that domestic context, although it is by no means the only measure of effectiveness.

While measures of effectiveness often include the prosecution of terrorist financing offences, this is by no means the only measure of effectiveness of FIUs and the prevention of terrorist financing. To effectively prevent a jurisdiction from being used for terrorist financing, law enforcement, security services, FIUs, and the private sector must work together to proactively identify terrorist cells and individuals that may be seeking to finance a terrorist plot. This is easier said than done because of the small data problem, but anomalous patterns of financial activity, combined with information that suggests that the individual may have radicalized and be interested in undertaking terrorist activity, can provide useful information to the financial sector to spot changes in behavior.

Indeed, information sharing with the private sector, either in the form of trends or typologies of terrorist financing, or in the sharing of more tactical, operational-level information, can provide valuable insight that can inform their understanding of suspicious activity. Much of this information is developed by FIUs, or is shared directly by law enforcement (including law enforcement style FIUs). Other measures of effectiveness include prosecutions of terrorist financing activities, which can include both operational and organizational financing by individuals within a specific jurisdiction, or the prevention of the establishment of entities for the purposes of terrorist financing. In some cases, prosecution may not be possible, but disruption of terrorist financing activities should still be considered a measure of success.

In some jurisdictions, the FIU has a very small role in the detection and prosecution of terrorist financing offences, and instead, law enforcement units take the lead on this activity.

\textit{Preventing and Countering Terrorist Financing (CTF)}

In terms of prevention, counterterrorist financing legislation, frameworks, and regulations fit within all three levels of prevention. In some cases, countering terrorist financing initiatives are aimed at upstream prevention, i.e., preventing the formation of a terrorist group or cell. Generally speaking, CTF initiatives do not prevent the formation of a terrorist group, but they can restrict the financing of the group, preventing the organization from expanding and being able to execute attacks. CTF initiatives may prevent the creation of terrorist cells (i.e., operational attack actors) by preventing the financing of the cell from the terrorist organization, but in reality, most cells (and indeed, individual attackers) self-fund a good portion of their attack plans (which often cost very little), meaning that stopping the financing of these cells and individuals falls squarely on domestic/local law enforcement or security services, with
little space for international CTF actors. What these initiatives do succeed at is forcing much of the financing of terrorist activity “underground,” potentially restricting the amount of funds that become available for operational activity, or at least making the transmission of those funds more challenging for terrorist actors.

Countering the financing of terrorism initiatives go some way towards providing some midstream prevention, such that restricting the financing of a terrorist group reduces the risk from the group or organization being able to prepare a terrorist campaign. Terrorist group actions are restricted by a lack of funds, or by a lack of ability to move, store, manage, or obscure those funds. As such, CTF can have an impact on midstream prevention. However, in practice, most terrorist groups, regardless of CTF activities aimed at them, have sufficient means to launch terrorist acts if not whole campaigns. Part of this challenge lies in the fact that many sources of terrorist funds are impervious to counterterrorism financing initiatives. For instance, many terrorist groups exploit the economic activity in the area where they are operating through taxation or extortion of funds from the local population. Restricting international financial flows or sanctioning those groups will have little impact on their ability to raise funds. Further, many terrorist groups employ money movement mechanisms outside of well-regulated sectors, using cash couriers or trade-based money laundering to move money for operational activities. As such, while counterterrorism financing initiatives may make it more challenging for terrorist actors to engage in their activities, for the most part, terrorist groups can adapt to CTF initiatives and launch their terrorist attacks or operational activity.

In terms of downstream or tertiary prevention, counterterrorist financing initiatives do little to help prevent operations or foil them in the traditional sense. Very few (if any) plots or attacks have been detected solely through financial intelligence and terrorist financing activities. However, the use of financial intelligence in investigations, including those that are not motivated by financial gain, is increasing. This financial intelligence can help investigators determine the level of planning and preparation of a terrorist cell or individual intent on undertaking terrorist activity, and correspondingly, help them to time their interventions or understand the capabilities of the terrorist actors. Financial intelligence, originally provided by FIUs, but now also obtained directly from banks and other financial institutions through warrants or other judicial applications, or in some cases, by established relationships with banks, is an increasingly significant source of information that can assist in terrorism investigations, beyond just financing.

Conclusion

There are many international bodies involved in preventing terrorist financing internationally. They focus on criminalizing terrorist financing, setting international norms for countering terrorist financing, and providing technical assistance for countries to implement these recommendations. At the national level, most countries have a FIU, and these domestic units interact through the Egmont group, and at multilateral meetings, and conferences hosted by many of the international counterterrorist financing bodies. This conglomeration of entities tackles upstream, midstream, and downstream prevention of terrorist financing with varying levels of success. Measuring that success, however, is not straightforward. While some measures insist on the number of prosecutions within a jurisdiction as a measure of countering terrorist financing effectiveness, in reality, these bodies make more subtle contributions that also need to be taken into consideration, including through the coordination and sharing of information. Ultimately, this sharing of information and any constraint in a terrorist group, cell, or individuals’ ability to finance their activity, be it at the organizational or operational levels, needs to be counted amongst the successes of the global counterterrorist financing regime. Without money, groups cannot operate, and even small cell or lone actor attacks can be constrained by a lack of funds. Countering the financing of terrorism may be one of the single
most effective ways to prevent significant terrorist attacks and activity: determining how best to do that, and how to measure those successes, remains a ongoing issue of concern.

Jessica Davis is an international expert on terrorism and illicit financing. She began her career in intelligence analysis with the Canadian Military, then transitioned to a policy role at Global Affairs Canada before becoming a team leader with Canada’s financial intelligence unit, FINTRAC. Ms. Davis’s last role in government was as senior strategic analyst at CSIS where she was responsible for terrorism financing issues and managing the Indicators of Mobilization to Violence project. Ms. Davis is now the president and principal consultant with Insight Threat Intelligence, and works to bring evidence-based solutions to the private and public sectors to counter illicit financing and terrorism. Ms. Davis has published extensively, and is most recently the author of “Women in Modern Terrorism: From Liberations Wars to Global Terrorism and the Islamic State” (2017).
Endnotes


3 Financial Action Task Force (FATF), ‘Who we are,’ FATF. Available at: http://www.fatf-gafi.org/about/.

4 This is a modified version of the framework used by the FATF. In 2015, the FATF described their model of terrorist financing; their typology focuses on the generation of revenue, the movement and use of funds, and the management of resources. Financial Action Task Force (FATF), ‘FATF Report, Emerging Terrorist Financing Risks,’ FATF, October 2015, p. 5; p. 11. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.


13 For instance, ETA was reported to have been involved in the drug trade as early as 1984. Other examples include FARC and the Shining Path. See also: Shelley, Lousie, Dirty Entanglements. Cambridge: Cambridge University Press, 2014, p. 109; Rollins, John, Sun Wyler, Liana, and Seth Rosen, ‘International Terrorism and Transnational Crime: Security


17 The Taliban is reported to have raised funds from wildlife poaching. Felbab-Brown, Vanda, ‘Making a Killing: The Nexus of Terrorism and Wildlife Trafficking,’ *Cipher Brief,* 7 December 2017. Available at: https://www.thecipherbrief.com/making-killing-nexus-terrorism-wildlife-trafficking#.WjmbXwdHp9c.twitter.


Toledo and Fabe 2018.


Clarke 2015, p. 51.

• Charities / non-profit organizations are believed to have been used by AQAP to obscure donations from international support networks. United Nations Security Council. Monitoring Team Report. S/2017/35 13 January 2017, p.11.


Ibid., paragraph 3(f).


Ibid.


FATF October 2020.

Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Council of Europe, European Treaty Series No. 141, 8 November 1990. Available at:


Financial Action Task Force (FATF), ‘Who we are,’ FATF. Available at: http://www.fatf-gafi.org/about/.


Financial Action Task Force (FATF), ‘Who we are,’ FATF. Available at: http://www.fatf-gafi.org/about/.

FATF October 2020.

Ibid., p. 11.

Ibid.

Ibid.


FATF 2019.


97 Egmont Group, ‘About,’ Egmont Group. Available at: https://egmontgroup.org/content/about.

98 Ibid.


101 Egmont Group, ‘About,’ Egmont Group. Available at: https://egmontgroup.org/content/about.

102 Ibid., p. 6.

103 Ibid., p. 22.


107 International Monetary Fund (IMF), ‘Anti-money laundering/combating the financing of terrorism (AML/CFT) assessments,’ IMF. Available at: https://www.imf.org/external/np/leg/amlcft/eng/aml2.htm.

108 Ibid.


110 Ibid., p. 193.


115 United Nations Office on Drugs and Crime (UNODC), Pakistan Office, ‘National Conference on Promoting Public-Private Partnership in Countering the Financing of Terrorism,’ UNODC Pakistan, 29 March 2019. Available at:
Ibid.

Ibid.


IMF 2004, p. 17.

Bibliography


Chatain, Pierre-Laurent, ‘The World Bank’s role in the fight against money laundering and terrorist financing,’ Int’l LFD Int’l, 6, 2004


Epatko, Larisa, ‘Everything we know about the San Bernardino shooting,’ PBS News Hour, 3 December 2015. Available at: https://www.pbs.org/newshour/nation/everything-we-know-about-the-san-bernardino-shooting.


Wells, David. ‘The United Nations and Counter-Terrorism,’ Talking Terror Podcast. Available at: https://soundcloud.com/user-366747443.
Web-based Resources


Egmont Group, ‘About,’ Egmont Group. Available at: https://egmontgroup.org/content/about.


Financial Action Task Force (FATF), ‘Who we are,’ FATF. Available at: http://www.fatf-gafi.org/about/.


International Monetary Fund (IMF), ‘Anti-money laundering/combating the financing of terrorism (AML/CFT) assessments,’ IMF. Available at: https://www.imf.org/external/np/leg/amclft/eng/amcl2.htm.


United Nations Security Council (UNSC), ‘Sanctions,’ UNSC. Available at: https://www.un.org/securitycouncil/sanctions/information

United Nations Security Council (UNSC), ‘Sanctions and Other Committees,’ UNSC. Available at: https://www.un.org/securitycouncil/content/repertoire/sanctions-and-other-committees


Chapter 15

Prevention of Cross-Border Movements of Terrorists: Operational, Political, Institutional and Strategic Challenges for National and Regional Border Controls

Sajjan M. Gohel

Securing borders is a realm of state activity that is frequently considered to be prone to vulnerability, especially in terms of how borders might provide opportunities for exploitation by terrorist actors. However, borders can also be utilized to disrupt and intercept terrorist threats. In crossing borders, terrorists potentially expose themselves to detection if their activities are properly monitored and recorded. It requires cooperation and collaboration between neighboring states, international institutions, and regional agencies. This chapter will begin by seeking to present three currently pressing regional situations that may reveal the most pertinent issues in terms of border security as these relate to terrorism. These are the European Union (EU) borders with Turkey and Syria as well as Africa, the southwestern border of the United States (US), and the Afghanistan-Pakistan-India borders. Next, it will analyze and evaluate political, institutional, and operational/technical obstacles to border security, specifically focusing on assessing the recently employed externalization strategy of the EU. The roles of immigration agencies, interagency cooperation, battlefield and military intelligence will also be examined, as well as technological factors and the usage of border walls.

Keywords: Afghanistan, border security, FRONTEX, foreign fighters, Mediterranean, Israel, Pakistan, returnees, terrorist infiltration, Turkey
Borders have traditionally been imagined by states, particularly in the contemporary globalized era, as sites of potential weakness. They are seen as permeable and vulnerable, generators of threat and risk. However, their utility for counterterrorism (CT) operations has, in some sense, been underplayed in the CT literature, which is more concerned with finance, tactics, recruitment, and ideology than with mobility. Transnational terrorists, by their very nature, require mobility in order to act. The challenges in countering terrorist infiltration across borders is significant. Strategies to prevent the cross-border movement of terrorists requires the need to first understand existing challenges and potential emerging threats.

Despite their perceived liabilities, borders are also locations of significant state strength. There are few other places, particularly in democratic countries, where the state is able to marshal a similar concentration of its own power in terms of technology, information gathering, official presence, enforcement prowess and surveillance capacity. Borders can be areas of vulnerability for terrorist organizations, especially when a comprehensive strategy is implemented to interdict, interrupt, and intercept terrorists and their plans through border security.

There are challenges, not least of which is that borders not only serve a security function. Any effective counterterrorism border security policy must consider the economic, political, and social roles borders play within and between polities. Borders are permeable for a reason. They are not designed to hermetically seal the states they encompass, and so the frequent refrain of “more” and “harder” border security can only take us so far before it contradicts and ultimately undermines other critical border functions.

Beyond this, the question of security cannot be considered absent from a context which includes human rights, international law, and politics. Border security is too often conceived exclusively through a security-focused lens, precluding a more holistic understanding. Any attempt to “solve” border security, quixotic as that quest may be, will not be successful if it is advocated for only within narrow institutional and cultural siloes. An additional dynamic is that some states use borders as part of their strategic statecraft to exert influence over its neighbors. By allowing terrorists to cross borders, the potential for inter-state conflict and further regional instability increases.

Moreover, transnational terrorism itself is an implicit rejection of fixed jurisdictional and political sovereignty. It works, in part, by operating in the jurisdictional gaps created among agencies and organizations, exploiting the complex patchwork of mandates, remits, and authorities that exist across and between modern states and their security organs. Working to prevent transnational terrorism therefore requires a coordinated and comprehensive approach which cuts across established institutional and professional divisions.

This is not a new insight. A call for genuine multilateral and multi-agency collaboration was a central message of the 9/11 Commission in the US and has been a common recommendation in the literature ever since. That this is much easier said than done is a similarly hackneyed observation, but until border security practice is coordinated effectively, both between states and the various agencies responsible for CT operations and border enforcement, it will continue to have relevance.

Another important aspect that may indelibly shape some parts of border security is the issue of public health, most recently in the form of the spread of COVID-19. Information infrastructures are even more crucial than before. Communicating risk factors and determining if terrorists are travelling from high-risk areas during pandemics, is difficult because the information and public health surveillance capabilities vary from country to country.

Based on interviews with dozens of border security officials, several common problems were identified:

- Substandard information sharing;
- Inability to comprehensively control the borders;
- Reactive rather than proactive approaches;
The Challenges

It is important to ascertain and comprehend three important dynamics that can either hinder or support more effective multilateral and multi-agency CT border security operations. These are political, institutional, and operational/technical dynamics.

Political Dynamics

As stated, effective CT requires, by definition, collaboration and coordination between various governments. Politics has historically presented a significant barrier to more effective coordination and remains so to this day. The limitations of politically-mediated CT effectiveness was best illustrated through the fraught partnership between Pakistan and the US in the “War on Terror.” Both the Bush and Obama administrations expressed frustrations about the inability of the Pakistani military to contain the cross-border infiltration of the Taliban into Afghanistan.

Another example is the Visegrad Group’s broad opposition to an increased mandate for the European Border and Coast Guard Agency (Frontex). The group, which included the Czech Republic, Hungary, Poland and Slovenia, have moved to block the expansion on the basis of national sovereignty and security concerns, arguing that border security should remain the prerogative and duty of sovereign states, rather than the EU. Hungarian President Viktor Orban stated that increasing Frontex’ mandate would strip Hungary of “its right to protect its borders” and that there was “no need for Frontex to protect the Hungarian border in our place.”

Political barriers to multilateral cooperation are intrinsic to the international system, and if border security strategies are made to be dependent on wholesale political change, they are unlikely to find success. This is not to suggest that politics is not a barrier to multilateral cooperation and more effective counterterrorism border security practice, but rather that the mechanisms through which political questions such as these will be resolved are distinct from those this chapter is primarily concerned with (this chapter focuses on the institutional and operational levels).

Ultimately then, while political tension and disagreement is the background noise against which almost all transnational CT operations are set, it is not the role of CT practitioners to address those problems. It is of course true that governments should work to address the political impediments to better border security, and that maximal effectiveness is impossible without it. The prescriptions here are both well-known and hard to achieve. A certain level of political constraint must be treated as a fundamental and inevitable aspect of the framework in which CT practitioners operate.

Institutional Dynamics

Ill-defined and cross-cutting institutional mandates and jurisdictional authorities are common features across CT focused border security. The European Border and Coast Guard Agency (Frontex) can again be used as an instructive example to illustrate this. Beyond the political challenges that Frontex faces, the size and scope of its mandate has been left, in part, unresolved by the agency’s expansion following the 2015 refugee crisis. Similarly, complex jurisdictional patchworks are evident in the US, where intelligence gathering, analysis, and enforcement responsibilities should ideally be shared by the police, FBI, state governments
and services, Department of Homeland Security (DHS), the intelligence services, Immigration and Customs Enforcement (ICE) and immigration services.5

Unclear jurisdictional responsibilities impede cooperation and information sharing by creating barriers to coordination. The problem can be exacerbated by issues of institutional mistrust and inter-departmental turf wars. Opposition to engaging with the legal technicalities of immigration service work combined with a general lack of trust in non-security personnel prevents the useful exchange of information between different agencies. Institutional blocks to effective coordination must be overcome in the border security context, where jurisdictional complexity and the presence of multiple government agencies is an essential part of the system.

Operational/Technical Dynamics

Even when agencies and governments overcome the political and institutional barriers to effective cooperation, they are faced with the practical questions of how, exactly, action can and should be coordinated. “Interoperability,” much like “multilateral action,” is talked about a great deal and very difficult to achieve. However, the lack of functioning technical and operational frameworks to knit together information collected, analysed, and stored by different agencies is a major impediment to improving CT border security.

Improving interoperability and technical effectiveness is critical because it is a protection against human fallibility. Border security agents frequently work under high pressure in time-sensitive environments where the requirement to check information against four or five separately held databases through separate IT systems and collated by a diverse array of agencies can be onerous. As a consequence, some countries fail to carry out systematic checks against Interpol’s databases as a vital part of their examination of refugee/asylum applications, for instance.6 Improving ease of use for frontline agents not only makes the border process more efficient, but it decreases the likelihood that mistakes will be made, and corners cut.

Existing Challenges and Emerging Problems

The Syria Legacy

From 2015 to the first quarter of 2016, around 920,000 people utilized the Western Balkans route to enter the EU, marking the height of the European refugee crisis in the region. The majority of migrants travelled via Greece or Turkey and then through Macedonia, Serbia, and Hungary. Since then, the number of migrants using the route has fallen drastically. Frontex estimates that 19,000 people travelled the Western Balkans route in 2017.7 This has been attributed to two factors. First, the signing of the EU-Turkey Statement in March 2016, which offered a liberalized visa process for Turkish citizens and around €6bn in funding in exchange for the closing of access to the EU for migrants travelling from Turkey.

Second, the hardening of borders by states on the eastern edge of the EU and transit countries along the route, which began with Hungary’s decision to build a razor-wire fence along its Croatian and Serbian borders in 2015 and was then subsequently extended in 2017.8 However, while the migratory pressure has receded from crisis levels, refugees were, by mid-2019, still travelling towards Europe through the region, although predominantly utilizing a different route that runs via Albania, Montenegro, and Bosnia and Herzegovina.9

The general migrant numbers do not tell us a great deal about the potential for terrorist-related activity. However, terrorist organizations such as ISIS have made active use of the 2015/16 crisis to infiltrate the EU. A number of terrorist operatives submerged themselves within the migratory stream of hundreds of thousands of asylum-seekers fleeing conflict-ridden and destabilized countries for Europe since 2011.10
However, these cases comprised a small number of the overall refugee population that entered Europe. Yet they do serve to highlight the ways in which overloaded border security and immigration apparatuses can be particularly susceptible to abuse by malicious actors in times of crisis. More broadly, Robert Leiken and Steven Brooke, in their analysis of the backgrounds of 202 known terrorists in North America and Europe from 1993 to 2004, reported that 23% of them had gained access to their target countries through asylum claims.11

Therefore, while the situation on the EU’s eastern border is no longer a “crisis,” significant questions remain about the capacity of the EU’s border security apparatus to resist further infiltration attempts, particularly if a new crisis were to occur, despite the EU’s increased investment in Frontex. By early 2020, prior to the spread of the COVID-19 pandemic, there were fears that a further exodus from Syria’s Idlib region could catalyze another crisis.12

Moreover, the situation has been exacerbated with the territorial shrinkage of ISIS, leaving thousands of returning Foreign Terrorist Fighters (FTFs) unaccounted for. In 2018, ISIS was estimated to have amassed a force of some 40,000 FTFs who had left their countries of origin to fight with the group, increasing the likelihood that FTFs will seek to enter the EU to carry out an attack.13 This is particularly salient when bearing in mind the ongoing strategic evolution of ISIS since the loss of its territory in Syria.

In dealing with potential FTFs that are detained in Turkey and Turkish-controlled areas in northern Syria, the procedures at the ports in informing the host nation are riddled in bureaucracy and resulting inconsistencies. This is in large part because the Turkish policing authority (Ishtibarat) and the migration authority responsible for the deportation of illegal residents are separate entities in Turkey.14 Quite often, EU countries are not getting informed in actionable time about potential returnees. Most EU countries resort to working closely with their diplomatic missions in Ankara and Istanbul, to learn about potential returnees when they appear at the embassy to request new travel documents.15

Lessons to be learned from border security problems faced by Turkey are the importance of gaining more detailed information on transiting passengers and the need for more comprehensive sharing of information. Additionally, it is also important to understand how FTFs travelled to Syria, who facilitated their evasion of security checks, as this provides also necessary information to control the return of FTFs.

The African-European Maritime Borders

During the COVID-19 crisis, the Schengen Borders Code provided EU member states with the capability of temporarily reintroducing border control at the internal borders in the event that a serious threat to public safety or internal security had been established.16 The reintroduction of border control at the internal borders was identified as an exceptional and short-term measure but deemed necessary to prevent the spread of the coronavirus.

The EU’s southern border is likely to come under more pressure in the short to medium-term. In 2018 alone, the number of irregular migrants reported to have entered Spain, either through its enclaves in North Africa, Ceuta, and Melilla, or by sea, more than doubled in comparison to the year before, reaching almost 60,000.17 Frontex noted in 2019 that “Sub-Saharan migrants could lead to new record in arrivals in Spain.”18

The rising popularity of this Spanish entry-point can, at least in part, be related to EU-backed measures elsewhere in the Mediterranean to make travel more difficult, including increased cooperation efforts with the Libyan Coast Guard. Similar to its policy on its eastern border, the EU has forged an agreement with Morocco which set aside €140m from its “EU Emergency Trust Fund for Africa” (EUTF for Africa) to help build Moroccan capacity to stem the flow.19

In CT terms, the situation is worrying for a number of reasons. First, and most important, is the growing terrorist threat in the Sahel. Al-Qaeda affiliate Jama’at Nasr al-Islam wal
Muslimin (GNIM/JNIM) operates across significant parts of Mali, Burkina Faso, and Niger while the Islamic State in the Greater Sahara (ISGS) has established itself in the three-borders region. In Burkina Faso alone, around 100,000 people have been forced to flee their homes to escape the growing violence.\textsuperscript{20}

This is in addition to the continuing operations of Boko Haram and other groups in Nigeria. While these organizations have, so far, demonstrated a predominantly local focus, two factors should serve as warning signs for officials. First, while the groups themselves are locally focused, they are affiliates of Al-Qaeda and ISIS, groups which have demonstrated a strategic objective of targeting Europe. Second, borders in the region are more statements of political intent than they are material realities, meaning the ability to infiltrate the EU by travelling north is that much greater.

Even if the focus of these terrorist organizations remains local, their capacity to generate migratory pressure has already been demonstrated. Large movements of people, even within the region, could create further conflict, as was the case with the destabilization of Chad due to the influx of refugees from the Darfur conflict.\textsuperscript{21}

Moreover, as research by Bove and Böhmelt shows, migration from terrorism-prone source countries affects the incidence of terrorism in receiving countries.\textsuperscript{22} The inherent weakness of borders across the region combined with limited state control capacity makes it likely that the Sahel and West Africa will continue to suffer from transnational terrorist violence, with the potential for that violence to migrate to other regions, such as Europe, via its southern land borders and the Mediterranean. The broader, and more elusive, danger is that destabilization will create crisis-level migration in neighboring states in the Sahel and West Africa – for countries with limited capacity to absorb the migratory pressure.

\textit{The US' Southwestern Border}

In 2019, US President Donald Trump pronounced in his State of the Union address that “the lawless state of our southern borders is a threat to the safety, security, and financial well-being of all Americans.”\textsuperscript{23} His statement is an expression of a historical concern with the Mexican border which can be traced to the 1980s, but has only been analyzed through the prism of CT since the events of 11 September 2001. However, despite the increased focus on the permeability of the border, if we look beyond the rhetoric, a different picture emerges.

A more nuanced picture is reflected in the CT literature, which is broadly ambiguous as to the specific threat posed by the openness of the southern border of the US by those referred to as “Special Interest Aliens” (SIA). Porous Latin American borders represent a possible entry point into the US. During the first half of 2018, US Customs and Border Protection reported six immigrants at ports of entry whose names were included on US government terrorism watchlists.\textsuperscript{24}

The primary agency assigned to SIA-interdiction duty was the US Immigration and Customs Enforcement (ICE) Office of Investigations, later renamed Homeland Security Investigations (HSI). HSI has some 240 agents in around 48 foreign attaché offices to pursue, disrupt and dismantle foreign-based criminal travel movements, especially those involved in the movement of SIAs from countries of concern.\textsuperscript{25} The SIA smuggling networks have proliferated alongside technological advancements in communication, transportation, and finance. The true degree of successful SIA undetected entries in the US is difficult to quantify.

There are various types of travel arrangements for SIAs. Todd Bensman identifies that one of the most important are the origin-to-destination journeys that are arranged in advance.\textsuperscript{26} They involve pre-existing shared relationships with a host of independent networks along the way. This comprises of initial contacting and the provision of travel documents, air tickets, accommodation, and transportation along each stage. Handlers take paying customers to other
handlers who then accompany them. Once the SIA reaches the US, other smugglers would meet and transport them to various cities.²⁷

Some smugglers have themselves even been able to guide SIAs across borders, often through passport-controlled airports outside of the US, and occasionally, inside the US. They are often kingpin smugglers due to their dual nationality. They often own or control a travel agency in Pakistan or Bangladesh, which recruits clients with misleading advertisements and through word of mouth. A subcontractor then provides fraudulent passports and purchases airline tickets.²⁸

The HSI is primarily concerned with the SIAs using origin-to-destination travel because of the role of the kingpins who control the cash flow, communications, relations with corrupt government bureaucrats, and take major logistical decisions such as when and where travel will occur.²⁹ The kingpins are businessmen working for profit. Most of the SIA networks depend on localized smuggling groups that are indigenous to a single country or region, such as coyote smugglers who shepherd people across the Mexican-American border. The use of local smugglers diminishes the personal risk of a kingpin being identified or captured, providing distance from SIAs as they move covertly.

**Afghanistan-Pakistan-India Borders**

Pakistan has been a locus of terrorist activity for several decades. The border security challenges between Pakistan and Afghanistan as well as Pakistan and India, are geographically and materially complex and made even more so by the political environment. Borders are only as strong as the states that want to enforce them, and they can only be as strong as the state wants them to be. The permeability of borders in the region to various terrorist organizations is at once a product of the general instability that characterizes many of the border areas and also a product of a more thoroughgoing political unwillingness to address border threats in a meaningful way. Border security between Afghanistan and Pakistan and between Pakistan and India has yet to achieve the bilateral political consensus necessary for proper enforcement to take place, particularly in a context in which unilateral action to enforce border security is hampered by conflict and state capacity.

This can at least in part be attributed to the historical origin of the borders in the region. The post-colonial settlement left a set of polities with conflicting claims to each other’s territory, as exemplified by the contestation of Kashmir and the Durand Line respectively since the late 1940s. The 1879 Treaty of Gandamak, signed in the midst of the Second British-Afghan War, led to the establishment in 1893 of the Durand Line as an arbitrary boundary between Afghanistan and colonial British India.

The Durand Line which is about 2,400 kilometres long and passes through a third of Afghanistan’s provinces, was drawn by a team of British surveyors, led by Sir Mortimer Durand. This contentious border, which remains in place today, split the Pashtun and Baluch peoples between Afghan rule and British colonial rule and thereafter, Pakistan.³⁰ Though the border is largely porous, the Durand Line followed the contours of convenient geographical features, as well as the existing limits of British authority, rather than tribal borders.

Since the Taliban were defeated and forced out of power in Afghanistan during Operation Enduring Freedom in November 2001, they used Pakistan as a sanctuary. Most of the movement’s leaders are settled there where they also meet and train as a rear base. The many crossing points between Afghanistan and Pakistan enable the Taliban to routinely slip over the border to carry out attacks against the Afghan government and civilians. They are rarely encumbered by anyone intercepting or stopping them.

On the Afghan side, portions of territory that Taliban fighters cross through is already under Taliban control. On the Pakistani side, areas near these crossing points were either lawless or manned by security forces who turn a blind eye to the Taliban’s activities.³¹ This is
in part due to the Pakistani military establishment’s policy of viewing the Taliban as part of its own strategic depth in Afghanistan.

It is estimated that there are over 200 crossing points between Afghanistan and Pakistan. Only two of them have border controls including immigration, customs, and security checkpoints in place. One is the Torkham Gate in eastern Nangarhar province and the other is the Wesh–Chaman Gate in the southern Kandahar province. The other crossing points are used by smugglers and drug traffickers as well as the Taliban fighting in Afghanistan.

The Taliban’s movements across the Durand Line are primarily along the southern zone, the Baramcha and the Badini crossing points, the first of which is located in Helmand’s remote Dishu district. The Badini crossing point is located in the Shamulzai district of Zabul province. Both crossing points are used by the Taliban for moving their fighters into Afghanistan and transferring their wounded back into Pakistan for medical treatment.

In 1999, the United Nations Security Council (UNSC) passed Resolution 1267 which established a sanctions regime to restrict the entry and transit of all high-ranking Taliban officials through their territories. This was later extended to include Al-Qaeda as well. The resolution called for Member States to “deny permission to any aircraft wanting to taking-off from or land in their territory if it was owned, leased or operated by or on behalf of the Taliban.” It also ordered a freeze of all financial resources that could benefit the Taliban.

In 2000, the resolution was amended to also include a prohibition on sales of military supplies to any territories controlled by the Taliban and a ban of entry and transit for all high-ranking Taliban members. These sanction measures were also meant for any organizations or individuals that have been tied to either network, the Taliban or Al-Qaeda, across the globe. The resolution was met with criticism due to claims of human rights violations, especially surrounding the listing and delisting procedures. For example, human rights groups expressed concern over a lack of right to an effective remedy, right to judicial review, right to a fair trial, and due process. In order to address these issues, two subsequent resolutions were passed: Resolution 1730 in 2006 and Resolution 1904 in 2009.

The Al-Qaeda Analytical Support and Sanctions Monitoring Team headed in 2011 by Richard Barrett reported that 32 states had not submitted reports on their implementation of Resolution 1267. His team also said in an evaluation that the resolution has “done little to constraint the operations and finances of listed Taliban.” More specifically, they state that the Taliban “have money and their assets are not frozen; they are reported to travel between Afghanistan and Pakistan and they have no shortage of weapons or other military-style equipment.”

Yet, some Taliban members have asked to be removed from the list so that they are able to take part in peace talks with the government, which “indicates that the sanctions do have some impact.” Glenda Juliano notes that where the sanctions regime’s power lies is in its ability to create an environment of cooperation and coordination amongst states to combat terrorist threats. As the evidence suggests, terrorists have and will continue to update and adjust their behavior in order to evade financial barriers.

Similar to the challenges in Afghanistan, cross border infiltration of terrorists and weapons into Indian-administered Kashmir is one of the key issues that causes friction between India and Pakistan. Additionally, it remains a key issue imposing cost on India in terms of deployment of military and paramilitary personnel for internal security. The areas of cross border infiltration are estimated to be a staggering 1,965 kilometres of land borders, which stretches from Pakistan-administered Kashmir, including the area of Gilgit-Baltistan, to Sialkot region in Pakistan’s Punjab region, which lies across Indian-administered Kashmir and India’s Punjab region.

Pakistan’s military establishment has, as part of its strategic statecraft, adopted a policy providing sanctuaries to internationally proscribed terrorist groups such as the Lashkar-e-Taiba (LeT) and the Jaish-e-Mohammed (JeM). The LeT and JeM are well trained and provided
with information about terrain. They possess real-time military intelligence regarding the presence of Indian border forces along the infiltration routes. Furthermore, they are fully trained and equipped with sophisticated military-grade communication equipment, which allows them to navigate safely and communicate with their handlers in Pakistan without getting detected. They also benefit from “cover firing” when Pakistani forces start shelling the Indian side to keep it engaged.

In many cases, there is a fusion of state negligence or complicity, compounded by the involvement of criminal networks. In the case of the Afghanistan-Pakistan border, as well the US’ southwestern border, stricter controls cannot be enforced at the border without hurting local livelihoods and fuelling local grievances about dividing families. The weakness of border controls is exploited by terrorists and criminal enterprise coupled with issues of capacity and corruption.

In all these cases, fully securing the borders is simply not achievable. Borders are too long, the terrain is too difficult, and will likely remain porous even in the best of times. This is especially true in the case of terrorist infiltration into Indian-administered Kashmir from Pakistan. It follows that improved border controls are unlikely to have a major impact on the complex security concerns of the border area that affect these regions. This is also partly because it suits the strategic agenda of the Pakistani military.

An effective CT strategy in these scenarios must be proactive and also understand the financial goals and structures in which terrorists operate, including their adaptive capabilities. Multilateral institutions must ensure compliance of nations with existing standards, while simultaneously seeking new and updated solutions sensitive to the evolving threat. The goal is not to just contain or reduce terrorism but to eliminate the flow of funds and capture the assets. While money laundering for criminals and drug traffickers is mostly for financial gain, for terrorists, the objective is not money but its use for committing acts of violence.

**Actions – Institutional and Operational**

**Multilateral Cooperation**

Multilateral cooperation on countering terrorism is as much a goal as it is a practical policy suggestion. It has been offered as a cure for a number of ills and has long been acknowledged as a critical component in the push to develop greater CT capacity. Significant progress was made with the unanimous passage of the “UN Global Counter-Terrorism Strategy” in September 2006. However, with more than a decade passed since then there is more work yet to be done in strengthening and deepening bilateral and multilateral partnerships, as pointed out during the 6th Review of the United Nations Global Counter-Terrorism Strategy in 2018.44

This section will review several proactive and pre-emptive measures that can be taken to improve multilateral cooperation efforts with regards to CT focused border security. It will be followed by an analysis of the EU’s recent agreements with Turkey, Libya, and Morocco and their viability as a model for a longer-term multilateral strategy.

First, there is the question of state capacity. Many of the most successful and long-term CT and security partnerships have been maintained between governments with significant state capacity. An example is the Five Eyes intelligence network, comprised of the US, the UK, Australia, Canada, and New Zealand. As Thoburn highlights, state strength is a pivotal factor mediating the permeability of borders, in addition to size, finances, terrain and politics.45

In short, stronger states tend to have stronger borders, and therefore increased ability to monitor them. However, much of the contemporary terrorist violence is concentrated in regions and in states which have historically struggled to police their frontiers. For example, with the
rise of terrorist violence in the Sahel, a region with thousands of kilometres of largely uncontrolled borders, the problem is only set to grow.

The UN’s Global Counter-Terrorism Strategy cites “building states’ capacity” as one of its four key pillars and states that the UN Counter-Terrorism Centre (UNCCT) may offer an institutional venue through which to drive capacity-building efforts. In 2018, the UNCCT carried out capacity-building activities in 61 countries, across 20 global, 12 regional and seven national projects.46 However, while the UNCCT’s funding nearly doubled between 2017 and 2018, from $14.7m to $26m, its resources are spread over a wide array of activities.47 With the diverse focus of the UNCCT, it may make sense to create new programmes concentrated on the need to build border security capabilities among partners, including projects addressing the use of collection and use of biometric data, advance passenger record information for airline travellers, and best practices on information-sharing.

The need for bespoke border security projects is compounded by the proliferation of organizations, entities, and actors that claim roles as stakeholders in setting the international CT agenda. As Alistair Millar notes, the profusion of different bodies, both national and transnational, tasked with implementing various aspects of CT policies has increased the likelihood that implementers “[lose] sight of what others are doing or have done.”48 This brings us to our second recommendation – the need to better clarify the jurisdictional remits of the agencies which play a role in CT-focused border security and to coordinate the division of responsibilities among them in order to ensure that their actions are “mutually reinforcing.”49

This, of course, is not a new insight. But its continued salience to border security is evident even from a cursory look at the weak spots of border security practice over the past decade. The failure to properly identify and delineate the role of immigration agencies and other non-traditional security actors within the CT framework was a contributory factor to the success of ISIS’ infiltration of the EU between 2015 and 2018.50

Finally, multilateral border security partnerships must be created strategically, with an eye towards future threats and the potential for current risks to evolve. CT operations are frequently reactive. As Wain argues, their reactivity is a defining aspect.51 This has certainly been true for many of the multilateral border security agreements reached in recent years. Both the EU’s 2016 deal with Turkey and its 2018 deal with Morocco were reactions to border security problems already manifest.

While reactive measures are certainly useful for partially arresting the migratory pressure caused by the civil war in Syria, such as the Turkey agreement, an overly narrow focus on a set of known, existing challenges leaves security apparatuses blind to future contingencies.52 In order to effectively counter terrorist cross-border mobility, states should look to ensure that they also sign multilateral agreements with those locales where terrorism is likely to emerge, not just where it already is.

The EU has made some strides in this area, most notably in June 2018, when the EU Council signed off on the Commission’s proposal to deepen CT collaboration and information exchange with eight countries - Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia, and Turkey.53

**Border Externalization as a Multilateral Counter-Terrorism Strategy**

In 2018, the EU provided €148m in migration-related assistance to Morocco, including €30m to improve border management in the Maghreb, €70m to support a crackdown against migrant smuggling, and €40m for a new border management system, all from the EUTF for Africa.54 The partnership echoed those the EU had forged with Turkey and Libya. In 2016, the EU and Turkey announced a new agreement, which gave Turkey €6bn in funding and a liberalized visa process for Turkish citizens in exchange for reducing the flow of migrants heading to Europe from Turkey. 2017 saw the signing of an EU-endorsed bilateral agreement
between Italy and Libya to fund the Libyan Coast Guard in order to capture irregular migrants seeking to cross the Mediterranean and return them to Libya. These deals can be read as acts of border externalization, attempts to outsource and externalize the operation of borders to foreign countries since Morocco, Libya, and Turkey have, in effect, been asked to police Europe’s borders.

Depending on one’s perspective, the deal with Morocco has been a success at the very least. The 2016 arrangement with Turkey has been widely credited, along with the hardening of border practices along the Western Balkans route, with ending the European irregular migration crisis and drastically reducing migratory pressure on Schengen Area countries. The operative word here being “European” – the humanitarian crisis that forced people to leave their homes has not ended, but merely Europe’s self-identified role within this crisis. Indeed, the UN estimated in 2018 that Turkey was host to around 2.9m refugees, a number disputed by Turkey, which placed the figure higher at 3.5m.

The Western Balkans route has become more cumbersome than it once was to prospective FTF’s travelling under the guise of asylum-seekers – but at the expense of genuine refugees seeking asylum in safer countries. Similarly, Italy’s partnership with the Libyan Coast Guard has been cited as a key factor in reducing migratory pressure in the central Mediterranean route. It is too early to come to any definitive conclusions about the efficacy of the Moroccan partnership, but with migratory pressure on Europe’s Western Mediterranean sea border and the Spanish enclaves of Ceuta and Melilla increasing, it would appear to have been a timely move.

Clearly, from a CT perspective, the short-term effects of the policy have had benefits, especially a reduction in migratory pressure which has led to increased levels of screening at the border, and an increased capacity of border agencies to focus on potential terrorism activities. However, the question these policies raise is whether border externalization can function as a longer-term strategy in the global fight against transnational terrorism.

It is certainly true that tackling the challenge of terrorist mobility will, by necessity, involve the application of policy instruments that also impact regular migration, as is the case here. Those sources which look to draw no link between migration and terrorism are overly optimistic and run counter to a growing body of literature identifying the correlations and connections between the two. Restricting migration is in theory a potential CT strategy because the fewer people allowed to use legal channels to cross a particular border, the lower the overall numbers of border crossings. Therefore, it is assumed that it will be harder for terrorist organizations and returning fighters to cloak themselves in the disguise of legitimate migrants. However, the real costs for this are paid by bona fide migrants.

Border externalization is one way of reducing migration. Since 2015, it has been the primary tool through which migratory pressure on Europe has been curtailed. Manjarrez argues that reducing “clutter” at the border, by which he means high levels of “chaotic” activity in border regions, exemplified by strong legal and illegal migratory pressure, should be a primary goal of border security policy, as “this same chaotic and cluttered environment makes the border vulnerable to exploitation by terrorist organizations.” Border externalization has succeeded in reducing “clutter” and in combination with Frontex’s new “Hotspot” policy, it has led to an increase in the screening rate at the EU’s borders to effectively 100% (more on this below).

However, a holistic approach to the formulation of policy at the intersection of migration and terrorism asks not only “how do we keep certain actors out” but “what happens to people after entry is denied”. To ask the first question exclusively is to think tactically, rather than strategically. The EU’s border externalization policies have been criticized for failing to deal with the humanitarian implications of this second question. Conditions in refugee camps in Libya have been singled out for their inhumane conditions, with reported human rights violations including “beatings by guards, gang rapes by armed men and forced labour.”
UNHCR spokesperson Charlie Yaxley stated in relation to migrants who had returned to Libya that “many report going hungry for days on end, not being able to receive urgent medical care that they require,” and noted that “Libya was not a safe place for vulnerable people on the move.” The Mediterranean has seen a significant rise in the number of deaths at sea due to migrant drownings, at least in part a product of the increased difficulty of entering the EU by other means. Despite the year 2018 seeing the fewest number of irregular migrant entries since 2013, it is estimated that around 2,275 migrants drowned or were reported missing while attempting to cross the sea.

Even if humanitarian abuses are set aside, the strategic costs of the current form of border externalization are potentially significant. The creation of refugee camps in terrorism-prone countries, filled with internally displaced persons and refugees from conflict zones and destabilized regions with significant terrorist organization presence, appears at face value to impede an overall reduction in levels of terrorist violence. The literature supports this view. This could be an opportunity for intervention through communication and outreach with those living in these camps, such as better training of staff on the ground regarding what to look out for in terms of potential recruiters. Moreover, Bove and Böhmelt find in their analysis of the link between migration and terrorism that migration from states with significant levels of terrorist violence can also affect the level of terrorist attacks elsewhere. Similarly, Choi and Salehyan state that “countries with many refugees are more likely to experience both domestic and international terrorism.”

A natural response would be to suggest that outright exclusion is therefore the order of the day – if refugees increase the likelihood of terrorist violence, then they should not be allowed to cross the border. The issues with this are twofold. First, it ignores humanitarian responsibilities incumbent upon states under international laws, which externalization policies avoid but do not negate. Second, it fails to acknowledge that refugees must go somewhere because they are fleeing some threat, and that a truly strategic approach considers not only the potential risks of accepting refugees but also the potential risks of not accepting them, despite the potential for the diffusion of terrorist violence and infiltration by FTFs.

Contemporary externalization policies have led to the creation of vast refugee camps in regions already prone to terrorist violence, and in at least one case, Libya, an active warzone. In the Afghan case, the experience in refugee camps in Pakistan was pivotal to the creation of the Taliban, and refugees provided a steady supply of recruits in the Afghan civil war. Border externalization is not a viable long-term CT strategy as currently constituted because it is a palliative, not a preventative measure. It is a short-term solution to a long-term problem, and it is potentially creating the conditions for further waves of terrorism, destabilization and violence.

Effective CT-oriented border security practice will need to look beyond the externalization of borders and the outsourcing of international legal responsibilities as a means by which to reduce the potential for terrorist infiltration in future.

The Role of Immigration Agencies

The contemporary concern with the link between migration, border security, and terrorism has created a renewed interest in the role immigration agencies can play in CT operations. National immigration agencies also have a role to play in sharing information, both with security services and within their own network of organizations, especially when it comes to terrorists who are unknown and not registered in any database. Common risk indicators are important to identify in order to increase the chances of detection of such individuals. In the words of Susan Ginsburg,
“A fundamental condition for effective policy planning is acknowledging that the largest group of trained government personnel already in position and actually available to detect foreign terrorists traveling to and hiding within the United States are not in the CIA, the FBI, or the military. They are in DHS and the Department of State.”

This statement is equally true for the European situation. Migration services can play two primary roles – as sources of intelligence, and as agents of enforcement.

The need for better integration of immigration officers into the CT efforts can also be shown through reference to the Paris 2016 marauding attacks network. One of the Iraqi suicide bombers who ultimately carried out one of the attacks was reportedly identified as suspicious by a Greek official on the island of Leros, where the attacker had stopped on his way to Europe. The individual did not spend much time with the other migrants. Arguably, it would not have made much difference if an intelligence officer had been present, unless the decision would have been to refer this individual for secondary screening and that would have been dependent on availability of resources.

Immigration agencies, along with border services, in many senses represent the “front-line” of the fight against transnational terrorism. It is highly likely that terrorists seeking to infiltrate target countries, unless they travel via illegal means, will come into contact with immigration officers before carrying out their attack. Partnerships with immigration agencies offer valuable opportunities to intercept and interdict terrorist plots before they happen.

This does not cover those terrorists who seek to gain access via illegal entry channels, but, as analysis has shown, many if given the choice do not. Of the 144 “terrorist asylum-seeker” cases identified by Sam Mullins, 78% had some sort of formal contact with the European asylum system, of which 21% had in fact been granted refugee status “or some other form of humanitarian protection.” Of the 78%, only 13% had their right to asylum denied. Just 16% had travelled within “irregular migrant flows” and had chosen not to register themselves with the relevant asylum authorities in their destination country.

It should be noted that in the absence of specific, detailed intelligence it can be difficult, if not impossible, to identify terrorists within the immigration system. In many of the cases mentioned above there were no indicators in terms of accessible criminal records or awareness of past affiliation that would have alerted authorities. However, better cooperation between police, intelligence, and immigration services may have created conditions to prevent the attacks or identity attackers earlier. In interviews with border officials, some detained individuals brazenly discussed their terrorist affiliations.

There are several barriers to better cooperation with immigration agencies, and they can be broken down into four main categories. The first, and theoretically most simple, is interoperability. The second is cultural, the third is capacity, and the fourth is awareness.

Interoperability, as previously noted, is a problem easy to identify and difficult to solve. Immigration agencies hold vast volumes of data and intelligence – the problem being that police and intelligence services may not have access to it, and when they do, it can be difficult to find and use. Improving interoperability between intelligence, border security, and immigration databases should be a priority for counterterrorism practitioners in the near future.

Cultural barriers to better cooperation exist because intelligence agencies have traditionally viewed immigration services and their border security cousins as “potential information liabilities.” Much like the “wall” that strategists identified after 9/11 in the US between the FBI and the CIA that prevented a holistic analysis of potential terrorist threats, the divide between intelligence services and the immigration policy and enforcement community is standing in the way of more successful CT operations in many countries.

Above and beyond classic inter-institutional rivalry and turf wars, which appears to characterize many interagency processes, the issues of culture and trust are hampering more
Effective communication and coordination between intelligence and immigration services. Whether this can be resolved at an institutional level is unclear. It may be necessary to create some sort of formal requirement that mandates information sharing in order to improve the exchange of data.

The challenge of capacity was most notable during the European refugee crisis. At points, the Bundesamt für Migration und Flüchtlinge [the German Federal Office for Migration and Refugees] (BAMF) lacked sufficient staff to conduct face-to-face interviews with all newly arriving asylum seekers. In some cases, individuals believed to be connected directly to terrorist plots had been granted refugee status after completing a questionnaire. The situation is much improved now with the reduction in migratory pressure, but increasing immigration agency capacity and providing targeted CT training and more liaison officers from other government branches tasked with CT operations remain a priority issue. As part of Germany’s push to improve immigration–CT partnerships, the government announced in 2017 that more intelligence officers were set to be stationed at BAMF field offices.

Finally, even when immigration agencies have been provided the funding, staff, and IT infrastructure necessary to work as functioning stakeholders within the CT border security process, lack of situational awareness can serve as a drag on effectiveness. European law enforcement agencies were in 2015 provided with only limited access to Eurodac, the EU’s Dublin agreement-based immigration database, initially created to determine which country would be responsible for handling specific asylum cases, after recognition that the information contained in the database would be of use to CT practitioners. However, in the first five months of access, only 95 searches were made by law enforcement, although this did increase to 326 searches over the course of 2016. Europol has had some challenges in being able to maximize the use of the database. Access does not equate to awareness, and maximal utility can only be achieved if the relevant officers on the ground are aware of the kinds of information stored in different immigration databases and their potential uses.

Interagency Cooperation and the Role of NATO, Frontex, Interpol and Europol

There are two kinds of interagency cooperation - national and transnational. National cooperation is that between different organs of the same government such as, in the case of the US, the FBI, DHS, and ICE. Transnational multiagency cooperation occurs below and above the level of multilateral partnerships between governments and requires the coordination of agencies from different sovereign states and international agencies and organizations such as NATO, Frontex, and Interpol.

This section will begin by reviewing the efforts of two organizations, NATO and Frontex, to explore the kind of roles that international and transnational agencies can play. They are important because transnational organizations and agencies such as these can function as critical partners and stakeholders in the interagency cooperation process, serving as central hubs connecting different spokes to serve as key coordinators of transnational interagency action. They provide an institutional mechanism through which information and expertise from a wide number of sources can be aggregated, synthesized, and analyzed.

The North Atlantic Treaty Organization (NATO)

NATO brings several advantages to the table, most notably military resources, political clout, and knowledge sharing systems. It would seem to be a natural venue through which to carry out and coordinate CT operations, and it has historically played a pivotal role as a central stakeholder in the global fight against terrorism. However, its utility in the border security
context may be limited by its military focus and member states’ desire to retain border security as a prerogative of sovereign states.

NATO was heavily involved in the Taliban in Afghanistan. NATO had attempted to make border crossing more difficult, but the Taliban kept bases within the civilian population inside Afghanistan. The Taliban had adapted by using civilian population centres and public facilities, such as existing health centres and schools, as cover.

In 2011, NATO unveiled its new “Alliance Maritime Strategy.” The document provided a mandate to NATO’s naval forces to “conduct surveillance and patrolling, share information, support law enforcement, enforce embargo and no-fly zones, and provide urgent humanitarian assistance and disaster relief.” In 2016, NATO launched “Operation Sea Guardian” in the Mediterranean, a “flexible operation” with four key tasks, including to provide “support to maritime counterterrorism.”

To achieve its CT objectives, Operation Sea Guardian involves close collaboration with Frontex and maintains information sharing partnerships with the Coast Guards of Greece and Turkey. In addition, the “Alliance Maritime Strategy” has contributed to efforts to assist governments with the response to the refugee crisis in the Mediterranean by providing reconnaissance and surveillance of illegal crossings of the Aegean. Beyond its maritime operations, NATO has also worked on border security-focused capacity-building projects in the Balkans and even in Central Asia.

The Alliance’s operations in the Mediterranean have been largely successful and played a role in reducing the number of irregular migrants travelling from Turkey to Greece. Stefano Marcuzzi has been arguing that Operation Sea Guardian has been tactically beneficial, contributing to enhanced situational awareness in the region. However, he cautions that the operation has had limited strategic effect, attributing this to a lack of information-sharing between the operation and non-maritime partners. He quotes an EU official, who stated that NATO’s maritime operations need to be considered in a broader context – “just an arrow in the quiver, not the only arrow we have”.

What is clear from NATO’s maritime contributions to CT-oriented border security is that, while it does have an important part to play, it can only do so much. As NATO’s own report acknowledges, border security is, and will remain, the primary prerogative of sovereign governments. Beyond this, the report concludes that border security is a political rather than military issue. While the line drawn here between politics and the military is perhaps overly stark, the point stands that the militarization of border security practice is unlikely to yield productive results over the long term, particularly bearing in mind the other functions, most importantly economic, that borders serve.

The European Border and Coast Guard Agency (Frontex)

Founded in 2005, Frontex is the EU agency responsible for the coordination of border control and border security efforts. Frontex, unlike NATO, has the potential to be a central stakeholder in CT border security operations due to its range of operations and breadth of jurisdictional authority. However, several barriers stand in the way of improved operational effectiveness, most notably ambiguity about the organization’s precise remit.

The agency is currently engaged in three projects worth mentioning here – capacity building (both its own and those of partner states), government partnerships, and interagency partnerships. In addition, Frontex runs three operations in the Mediterranean with CT components – “Indalo” in the west, “Themis” in the centre, and “Poseidon” in the east.

- **Capacity Building:** Frontex is pushing to use less equipment loaned from member states as part of a broader effort to increase its own capacity. The push has, at least in part, been inspired by experiences of the European refugee crisis of 2015, which
highlighted the need to bolster the agency’s capabilities in preparation for future crises. Observers have noted that the agency continues to rely strongly on voluntary contributions of equipment and personnel from EU states in order to carry out its operations, despite its recent funding increases. To this end, the EU had also moved to increase Frontex’s staffing numbers from 1,500 to 10,000 by 2020, although the completion date has been pushed back to 2027.

- **Government Partnerships:** Since 2015, Frontex has been working to build partnerships with third countries, particularly those on the EU’s outer border, to help improve their border security operations and capabilities. In 2017 and 2018, the organization signed “status agreements” with several states in the Balkans, including the Republic of North Macedonia, Serbia, Albania, and Montenegro. This allows the agency to deploy its employees there. Frontex itself highlights the efforts, noting that “wide-ranging cooperation with third countries has proven to be paramount in order to improve the effectiveness of border controls.” Further Frontex has also stationed 11 liaison officers across the EU to “enhance the cooperation between the Agency and national authorities responsible for border management, returns and coast guard functions.” However, despite Frontex’s partnership initiatives, the organization faces pushback within the EU. The Visegrad group in particular has opposed the expansion of the agency’s mandate, on the grounds that it represents a challenge to a sovereign responsibility of individual Member States.

- **Interagency Partnerships:** In addition to efforts to improve cooperation with national immigration and border services, Frontex has also deepened its collaboration with Europol in recent years. Frontex and Europol jointly developed a handbook, regularly updated, which is designed to raise knowledge and awareness among frontline staff, who will then be better equipped to identify possible signs of involvement in terrorism. In 2018, Frontex and Europol announced a new agreement to “expand the exchange of information between them to strengthen their joint fight against terrorism and cross-border crime” with a focus on “identifying complementary capabilities and expertise at Europol and Frontex and improving cooperation on the ground.”

These three projects have fed into the development of Frontex’s “Hotspot” strategy. Hotspots refer to those areas of the European border faced with extraordinary situations or crisis-levels of migratory pressure that are determined to require additional support from relevant EU agencies. Frontex and Europol have together deployed more than 200 officers as part of the strategy, with a particular focus on Greece and Italy. They have primarily been tasked with assisting with the screening of migrants through registration, fingerprinting, and debriefing. These deployments have been credited with an increase of migrant screening rates at the European border to nearly 100%.

However, despite Frontex’s success in contributing to the CT border security effort, the agency still faces several barriers hindering its success – most importantly, jurisdictional and legal ambiguity regarding the precise scope of its mandate.

Frontex has undergone several expansions in the course of its short existence. Established with a relatively limited mandate, Frontex was already moving into new areas by 2007 with the creation of “Rapid Border Intervention Teams” designed to provide swift assistance to the border forces of member states facing significant pressure. The 2015 refugee crisis represented the turning point in the agency’s history, and provided further impetus for its growth, exemplified by the agreement of EU States in 2016 to establish the European Border and Coast Guard Agency (EBCGA), dubbed ‘Frontex+’. Frontex was provided with a larger budget, new capabilities, including the mandate to organize return flights for illegal migrants, and an expanded slate of responsibilities. However, the negotiations to expand Frontex left several
questions unanswered, including the legal specificities surrounding its “right to intervene” in an EU Member State without the state’s express permission. The issue was ultimately resolved with a compromise that allowed the EU to “re-introduce internal border controls aimed at those member states unwilling to cooperate with Frontex in a migration crisis.”

However, the case remains that Frontex’ authority in its current incarnation is contestable and contingent on the support of states. As long as its status as a legitimate actor can be, and is, called into question by a number of EU member states, its capacity to play a role as a central coordinating body in CT border security is limited. However, even with these constraints, Frontex’s efforts in recent years demonstrate that it is a strong candidate for such a role, along with Europol and Interpol, and may be better suited than these due to its narrower focus on questions of border security and migration.

**Battlefield Intelligence and Military-to-Law Enforcement Information Exchange**

The efficacy of biometric identity systems, advanced passenger information, passenger name records, fingerprint registration, and criminal records checks is almost entirely dependent on the quality of the content of the data in various databases. Databases themselves are restricted by locale, agency, and bureaucracy. A European criminal records check can only do so much when assessing the asylum claim of a refugee who has never before been to Europe. The traditional way to overcome this deficit is multilateral information sharing, forging strong partnerships with source and transit countries to close information gaps.

This leaves one glaring hole - migrants from destabilized and conflict-ridden countries of origin. For example, it would be very difficult for Frontex, Interpol, or the FBI to partner with the Syrian state. Similarly, in countries where the state structure has broken down, even if a partnership were possible, the information provided would likely be of minimal value. War zones can act as identity launderers for those that emerge from them – records get lost or are destroyed, leaving CT investigators unable to track the individuals inside such states.

That this is a critical vulnerability is evident when we consider the Paris-Brussels terrorist network and the broader body of terrorist cum asylum-seekers who gained entry to the EU between 2011 and 2018. Two members of the group that went on to carry out the attacks in Paris in November 2015 underwent screening, fingerprinting, and had their photographs taken by European authorities before continuing their journey on towards their target country. Over a dozen attacks have been carried out since 2011 by terrorists who claimed asylum in Europe during the 2015 mass migration crisis and an additional 24 attacks were averted. As noted above, 78% of all terrorist asylum-seekers identified in Mullins’ study had some sort of formal engagement with the asylum system. That they were not flagged is, in part, an operational and institutional failure, but it is also a product of the inherent limitations of the information contained in CT, law enforcement, immigration and border security databases.

Refugee crises are unlikely to emerge from peaceful, functioning states. Crises represent significant opportunities for terrorist infiltration, particularly when they are, in part, products of terrorist violence in countries of origin. There remains a need to try and improve the flow of information from conflict zones more directly. Valuable intelligence gathered from the battlefield could prove to be decisive in disrupting terrorist cells and structures that operate across borders. Data on FTFs held by multilateral organizations and which is sourced from conflict zones need to be supplemented with military-to-law enforcement information exchange in support.

This is not a novel proposal. Interpol has pushed military-to-law enforcement information exchange since 2005 with its “Project Vennlig” in Iraq and, later, “Project Hamah” in Afghanistan. In 2017, the EU’s Counter-Terrorism Coordinator put forward a set of proposals for improved “military, law enforcement and judicial information exchange in counter-terrorism,” arguing that information gathered by militaries
“could have an immediate operational value, because it would enable authorities to stop fighters trying to cross borders (especially re-entering Europe from the battlefield), to dismantle their networks and supply chains in order to weaken their warfare and to prevent attacks in Europe. It may also have judicial value in helping to bring terrorists to justice.”

In October 2017, Europol confirmed the deployment of an analyst to a law enforcement cell in “Operation Gallant Phoenix” to process fingerprints and DNA data collected by the US military. The US has, since 2001, deployed law enforcement personnel as part of military operations to facilitate the collection of evidence, and both the US and Canada train their military forces in proper evidence collection procedures.

The training of armed forces is in fact critical if battlefield evidence is to be utilized as part of CT investigations. Paulussen and Pitcher note that frameworks must be put in place to ensure that military personnel collect and handle evidence in such a way as to allow it to be admissible in civilian courts. While inadmissible information may be enough to deny entry at the border, should information be gathered once an individual has entered a particular country, any evidence will need to meet the legal standards of that state.

One must also look beyond law enforcement-to-military exchange in the field of border security and integrate immigration agencies and border forces. If, as stated above, immigration and border services form part of the frontline fight against terrorist mobility, then they have to have some form of access to military evidence in order to operate effectively in identifying terrorist risk and suspicious individuals.

**Actions - Technological**

The proposal of technological solutions to border security challenges has a long, and not particularly illustrious history. Take President George W. Bush’s “Secure Border Initiative.” Described by the president as the “most technologically advanced border security initiative in American history,” the plan was to equip the US’ 6,000 miles of land border with a series of towers, sensors, and cameras. According to the project’s corporate manager, Boeing, the new array of high-tech equipment would be able to detect 95% of all irregular border crossings. Unfortunately, the sensors did not work as hoped. They misidentified raindrops and leaves as migrants, and the “Secure Border Initiative” was ultimately cancelled in 2011. 53 miles of border had been fitted with the technology, at a total cost of around $1bn, working out at around $19m per mile.

Donald Trump and his supporters have claimed that expanding the barrier between the US and Mexico or “building the wall” will cause a dramatic decrease in crime and illegal immigration for the US. However, experts disagree, as studies conducted since 2016 have undermined those assumptions.

For example, a 2018 paper authored by economists from Dartmouth and Stanford found that building a wall at the US-Mexico border actually served to result in economic harm for US citizens and did not significantly reduce migration (only by 0.6%). Migrants simply altered their routes, though they were more difficult, and the cost for US taxpayers was substantial—approximately $7 per person. Higher skilled American workers lost around $4.35 in their yearly income, and lower skilled workers gained only 36 cents. This study focused on the consequences of the Secure Fence Act of 2006, which cost $2.3 billion and added 548 miles of fence. Instead, the authors suggest, other solutions should be explored that address the root of why people migrate: lowering trade costs between the US and Mexico, for example, would result in economic benefits for both countries’ citizens, they predicted.

Regarding the threat of terrorism, there is no current evidence suggesting that active terrorists have entered the US over US-Mexico border. However, that cannot be ruled out,
particularly when considering SIAs. There has been evidence that of smugglers working with entities that have connections with Jihadist entities to bring people into the US, although the purpose may not have been terrorism but other clandestine activities. Michael Dear, a professor of Geography at UC Berkeley, has noted that cartels can actually use the limited number of ports of entry to their advantage due to their predictability. They can observe and more precisely target points of weakness or particular security officers in order to continue smuggling goods across – and in tunnels under - the border.

That this is not the fate of all border security technologies is of course true. However, the “Secure Border Initiative” should perhaps serve as a cautionary tale – technology is not a panacea, nor can it serve as a total substitute for other forms of border security. Further to this, technology such as that installed during the project is often faced with a choice between responsiveness and accuracy. One can almost capture 100% of activity, and therefore force border agents to respond to multiple false alerts, or one can have increased accuracy, which runs the risk that individuals might slip through undetected. While the development of AI promises an end to the responsiveness/accuracy dichotomy, there is little evidence to suggest that it has solved the challenge completely, at least as of now. As Jack Riley noted, “[t]echnology is not a substitute for trained, professional security personnel.”

However, with this in mind, there are a number of CT focused border security technologies which are being productively deployed and should be expanded on. Biometric information gathering, improved databases, camera technology for face recognition, pressure sensors, drones, and license plate readers are some of these technologies, although these too can be tricked and misused.

Although technology greatly supports border security, it cannot phase out human observations and intuition. Overreliance on technology for security processes will condition border guards to depend on computer systems for daily tasks. However, these systems cannot reveal the intent of travellers. Technology needs to accompany human intelligence and behavioural cues. Border security also requires real-time information from staff stationed at embassies and consulates abroad who can provide valuable information about societal and political developments that could impact on other countries.

Ultimately, technology’s utility is directly related to its ability to be deployed in ways that enhance, rather than detract, from the capacity of border security personnel. When used incorrectly, it can contribute to “clutter” in border zones and drain valuable time from officers tasked with investigating false alarms and faulty sensors.

The Benefits and Disadvantages of Border Walls

In his report, Lord Jopling has presented Israel’s West Bank “smart wall” as a potential example of best practice in the field. Equipped with a layered set of “sensors, radar, and cameras,” the fence is reportedly able to distinguish between people and plants or animals. A cautionary note should be sounded here – while Israeli technology may be world-leading, its border is, comparatively speaking, short, and there may be questions about the technology’s capacity to be extended over a longer area.

Looking back, the second intifada, which lasted from September 2000 to February 2005, coupled with the proliferation of suicide attacks by Palestinian militants, led to the creation of Israel’s West Bank barrier or wall/fence in 2002. Advocates of Trump’s border wall with Mexico point to its success in order to suggest that similar positive effects would result from expanding the US-Mexico wall. However, each respective situation involves different circumstances. Moreover, other factors may have played into the decrease in suicide bombings in Israel alongside the construction of the West Bank wall/fence.

Israel was facing a severe uptick in suicide bombings by 2001. The following year, Ariel Sharon ordered the construction of the border wall/fence with the West Bank. In doing so, he
went beyond the 1967 borders, thereby effectively annexing further parts of the West Bank.\footnote{114} This was met with international disapproval, yet Israel stood by the decision due to the barrier’s perceived effectiveness to significantly lower suicide bomb attacks. In 2002, the Israeli Ministry of Foreign Affairs and the Shin Bet security agency reported that there were 452 fatalities from attacks.\footnote{115} After the completion of the first continuous segment through the end of 2006, the attacks emanating from the West Bank, killed only 64 people.\footnote{116} Attacks continued to decline thereafter.

Al-Aqsa Martyrs’ Brigades, Hamas, and the Palestinian Islamic Jihad have been less able to conduct attacks in Israel. Suicide bombers from the northern West Bank would have to travel much further in order to get around the wall/fence. Israeli intelligence capacities had also increased, and the effort required for would-be suicide bombers may have acted as a deterrent. However, the wall/fence has been met with serious backlash from Palestinian villages nearby with weekly demonstrations to protest the wall, and ensuing violence between the protesters and the Israel Defence Forces (IDF).

The case for a wall for the southwestern border of the US tends to be made on two grounds, intuitively, and through reference to studies on the San Diego and Yuma sections of border wall constructed there. The first ground is subjective as intuition is not a sufficient justification on its own for the outlay of billions of dollars. The second, evidence-based argument, is more complex, but the weight of analysis ultimately suggests that, in most cases, border walls are unlikely to be the most effective way to spend border security or CT funds, and their overall ability to fulfil on their exclusionary promise requires further primary research.

In the mid-2000s, the US government constructed walls along the border with Mexico near the Arizonan city of Yuma. The fencing there reportedly led to a decrease in border apprehensions of 90%, and a similar effect was found in San Diego following the building of a wall to the south of the city in the 1990s.\footnote{117} However, while crossings in those particular areas which saw wall construction did fall, the overall effect was merely to force migrants to attempt to cross at more dangerous points.\footnote{118} The Migration Policy Institute found that the number of migration-related fatalities recorded at the Tucson morgue rose from 18 per year in the 1990s to nearly 200 per year.\footnote{119} Analysis by the US Government Accountability Office has not been able to show that the construction of physical barriers improves border efficiency – if anything, their study has found the opposite. From 2013 to 2015, there were more arrests on those sections of the border which already had fencing.\footnote{120}

Estimates on the cost of building a wall on the US’ southern border varied significantly, ranging from $12bn to $70bn. For comparison, the construction of 650 miles of fencing during the George W. Bush administration cost the American government $7bn.\footnote{121} Part of the variation is attributable to disagreements over the exact kind of barrier that the border calls for – whether concrete slabs, mesh wire or steel fencing. The Trump administration had not conclusively settled on the issue. Its record on constructing new walls (rather than merely fortifying existing ones) was poor and marred by corruption. The Biden administration largely abandoned the border wall project in early 2021.

One challenge prospective wall-builders face is that walls are expensive, and ladders and tunnels are cheap. Border security is more effective when there are programmes that stem from the points of origin, rather than trying to mitigate a problem at a point of the border. It remains unclear to what extent border walls can be considered effective, and, even if they were, the question remains of whether it actually permanently resolves a problem or only contributes to an already existing humanitarian crisis. Pakistan’s unilateral installation of a wall on its border with Afghanistan has created social, economic, political, and military tensions. Its border management plan, launched in 2017, aims for a divider along the entire Durand Line.\footnote{122} The theory is that the fencing will disrupt militants plotting attacks from Afghanistan. However, if Pakistan’s goal in Afghanistan remains ‘strategic depth’, the border wall could serve as a tool to control the traffic of militancy ensuring it only goes one way, into Afghanistan. Worse still,
farming and cross-border trade were among the only sources of income for many people along the border. The wall has separated thousands of families who share the same culture, traditions, language, religion, and ancestral land. As security issues become more politicized and trade and travel expand, despite the challenge of pandemics, sealing borders is not a viable solution. It simply pushes terrorist threats underground and causes additional problems in the future. Since intergovernmental issues require intergovernmental solutions, border security involves all community stakeholders both inside and outside the “walls.”

Conclusion
Borders serve more functions than merely security alone. Borders also have symbolic, political, as well as material functions. Harmonizing these is not an easy task, especially in the COVID-19 environment and the potential legacy it might create. It is certainly not a task accomplishable by CT professionals or border security personnel alone. Instead, participation from, and cooperation between, states and intergovernmental organizations along with immigration agencies and military intelligence must be emphasized as well.

Protecting a nation’s borders from the illegal movement of weapons, drugs, contraband, and people, while promoting lawful entry and exit, is essential to a country’s national security, economic prosperity, and sovereignty. The mission of a nation’s border control, security, and management system is to detect and prevent illegal aliens, terrorists, and weapons from entering a country, and prevent illegal trafficking of people and contraband.

To better prepare, prevent, and disrupt terrorist and terrorist-related travel, countries need to strengthen national identity management chains, from the delivery of reliable breeder documents, such as birth certificates, to the safe and reliable issuance of secure identity and biometric travel documents. Government authorities should constantly evaluate and improve the integrity of their country’s identity documents, issuance procedures, inspection processes, and management systems with a focus on promoting effective, robust, and internationally compliant measures. With the adoption of UNSC Resolution 2396, the UN identified three crucial border security elements: appropriate screening measures at the borders and enhancing identity management; enhanced collection of passenger data and biometrics; and increased information sharing, both among states and within states.

Terrorists seek to operate anonymously to evade detection, by blending into civilian populations, traveling incognito, and using false names for stealth. As such, in addition to having robust border security protocols and properly resourced and trained border officials, national authorities should also develop identity management capacities and protocols. Coupled with robust training and human intelligence, identity information capabilities, including biometric enrollment and screening systems, forensics results, and identity intelligence, are effective tools in detecting threat actors and support networks. Sharing timely identity information among border security, law enforcement, military, and security services, as well as with regional and international partners and appropriate multinational organizations is key to providing enhanced national security and constitutes the fundamental principle of defense-in-depth.

With the adoption of UNSC Resolution 2396 in 2017, the UN has advocated a series of measures aimed at helping States to prevent the transit of terrorists. The resolution has three key border security elements: 1) appropriate screening measures at the border checkpoints and enhancing identity management; 2) increasing the collection of passenger data and biometrics; and 3) improving the sharing of information, both among states and within countries. It is likely that, due to limited capacity and resources, governments will require several years to adopt all these border-related measures. In this context, regional and international organizations have started to play a key role in raising awareness and promoting the
implementation of Resolution 2396, and in providing operational and legislative assistance to states.

Unfortunately, some rogue states choose to engage in state-sponsored terrorism, involving intentional state support for terrorist acts of violence, either through direct support for the act itself or to support and maintain the survival of terrorist organizations. Where it comes to countries engaged in cross-border terrorism, private sources of financial and logistical support for terrorists must be subjected to the full force of international laws and under the purview of multilateral organizations such as the Financial Action Task Force (FATF). More needs to be done by other organizations engaged in monitoring and intercepting terrorists travelling across borders to collaborate with the FATF and the International Monetary Fund (IMF) to crack down on terrorist groups that attack other states.\textsuperscript{124} The need for improved cooperation and exchange of information relating to terrorism suspects, in particular with source and transit countries is a work in progress and if it continues to remain an obstacle it will hinder the ability of countries to control the situation. Bilateral and multilateral security cooperation agreements provide a legal basis for the exchange of personal data and the prosecution of those who are arrested.

One attempt at this is the EU’s recently employed tactic of border externalization. Yet, like border walls, it acts as a temporary rather than a permanent solution that could address issues at their origin. Once again, broadly speaking, interoperability is key, although certain factors, especially political ones, can hinder this, and it is difficult for CT practitioners to have much influence in this sphere. This includes enhanced intelligence sharing strategies among the aforementioned entities and more systematized methods of communication.

Furthermore, risk analysis must be done carefully, so as not to fall into the trap of racial profiling, which can lead to further marginalization and alienation of communities. Human intelligence is an essential component such as tip-offs from within the migrant community. Securing borders and enhancing both international and domestic cooperation are important but cannot function without frontline human intelligence.

An on-going legacy from Iraq and Syria will be that many FTPs may flee to other countries of armed conflict, such as Libya and Afghanistan - countries which do not have strong border patrol measures in place. This could provide the opportunity for the renewal of the jihadist movement’s growth. Moreover, terrorist groups’ ability to create and distribute fake travel documents - often with the help of organized crime, should not be underestimated. Borders and their control will remain a challenge for years to come.

\textit{Dr. Sajjan M. Gohel has a multi-disciplinary background in global security issues. Dr. Gohel’s current research includes looking at the ideologies and doctrines that feeds international terrorism, the varying tactics and strategies of trans-national political violence, border security challenges, and the role new media play for strategic communications. As International Security Director for the London-based Asia-Pacific Foundation, a policy assessment think-tank monitoring emerging geopolitical threats, Sajjan acts in a consultancy role for law enforcement agencies, foreign ministries and defence departments, multilateral organizations, universities, NGOs and the international media. Sajjan Gohel has also provided in-depth reports on security issues to the European Union, UNHCR, NATO, OSCE and INTERPOL. Sajjan’s research is case-study driven and he has fieldwork experience in 23 countries. Sajjan has provided expert witness testimony to numerous political standing committees on the evolving challenges and threats in Afghanistan-Pakistan, North Africa and the Middle East. In his role as Senior Advisor to the Partnership for Peace Consortium’s Combating Terrorism Working Group (CTWG), he heads its programme development on countering violent extremism. The CTWG is a collaborative research project investigating current transnational security threats and comprises of members from over 30 countries and}
multilateral organizations. Sajjan received his BA (Hons) in Politics from Queen Mary, University of London. He also holds both a Master’s degree in Comparative Politics and a PhD in International History from the London School of Economics & Political Science (LSE) entitled, “Insurrection of the Ideologues: The Evolution of Egyptian Islamist Radical Ideological Thought from Hasan al-Banna to Ayman al-Zawahiri.”

Acknowledgement

The author wishes to thank Victoria Jones and Henry Wisbey-Broom for their assistance in helping to research this chapter.
Endnotes


4 Angelescu, Irina and Florian Trauner, ‘10,000 border guards for Frontex: why the EU risks conflated expectations,’ European Policy Centre, 2018.


7 Jopling 2019, p. 4.


9 Interview with Border Security official from Bosnia-Herzegovina, 24 July 2019.

10 Interview with Frontex official, 25 June 2019.


14 Interview with EU law enforcement officials 24 September 2019.

15 Ibid.


27 Ibid.
28 Ibid.
33 Ibid.
34 Ibid.
36 Ibid.
39 Ibid.
40 Ibid.
41 Ibid.
42 Juliano 2020.
47 Ibid., p. 2.
49 Ibid., p. 7.
50 Interview with EU Border Security official, 15 September 2019.
51 Wain, Matthew, ‘Counterterrorism and Homeland Security are not the same Thing,’ Just Security, 4 March 2019. Available at: https://www.justsecurity.org/62776/counterterrorism-homeland-security/.
58 Interview with Border Security official from Bosnia-Herzegovina, 24 July 2019.
60 Ibid.
61 Interview with EU border security official, 23 August 2019.
62 For instance, Bove and Böhmelt 2016.
64 Mullins 2019, p. 122.
68 Bove and Böhmelt 2016 p. 574.
69 Choi and Salehyan 2013, p. 53.
71 Interview with Frontex official, 25 June 2019.
73 Interview with EU border security official, 23 August 2019.
74 Ginsburg 2006, p. 102.
75 Mullins 2019, p. 125.
76 Interview with EU border security official, 16 May 2019.
77 Mullins 2019, p. 128.
78 Interview with Europol official, 9 March 2019.
81 Interview with NATO Official, 2 February 2019.
82 Ibid.
84 Jopling 2019, p. 15.
85 Frontex, ‘2018 in Brief,’ Frontex, 18 February 2019, p. 3. Available at: https://frontex.europa.eu/assets/Publications/briefreport2018/.
86 Angelescu and Trauner 2018, p. 2.
87 Jopling 2019, p. 12.
93 Interview with Frontex official, 25 June 2019.
94 Angelescu and Trauner 2018, p. 2.
95 Ibid.
96 Interview with Frontex official, 12 November 2017.
103 Ibid.
104 Ibid.
106 Ibid.
107 Ibid.
108 Ibid.
113 Jopling 2019, p. 4.
118 Etter and Weise 2018.
119 Ibid.
120 Jopling 2019, p. 3.
Bibliography


Angelescu, Irina and Florian Trauner, ‘10,000 border guards for Frontex: why the EU risks conflated expectations,’ European Policy Centre, 2018.


Barigazzi, Jacopo and Randerson, James, ‘What is Europe's migration fight about?’ Politico, 22 June 2018. Available at: https://www.politico.eu/article/europe-migration-crisis-fight-explained/.


Paulussen, Christophe, and Kate Pitcher, ‘Prosecuting (Potential) Foreign Fighters: Legislative and Practical Challenges,’ International Centre for Counter-Terrorism (ICCT), 2018.


Wain, Matthew, ‘Counterterrorism and Homeland Security are not the same Thing,’ Just Security, 4 March 2019. Available at: https://www.justsecurity.org/62776/counterterrorism-homeland-security/.


Web-based Resources

Europol. Available at: https://www.europol.europa.eu/organisations/european-border-and-coast-guard-agency-frontex
Frontex. Available at: https://frontex.europa.eu/
Interpol. Available at: https://www.interpol.int/en/How-we-work/Border-management.
OSCE Border Management Staff College. Available at: https://www.oscebmsc.org/en/news.
US Border and Customs. Available at: https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics
Chapter 16

Prevention of the Procurement of Arms and Explosives by Terrorist Groups

Mahmut Cengiz

This chapter analyses how to prevent the procurement of arms and explosives used by terrorist organizations. It defines arms and explosives broadly, ranging from conventional arms to improvised explosive devices (IEDs) and close combat weapons. It explains key factors that lead to the creation of favorable environments for terrorist groups to gain access to arms and explosives. With a focus on terrorist groups who have perpetrated frequent attacks, the chapter showcases the jihadist and Maoist groups and their commonalities in terms of procurement of arms and explosives. Finally, the chapter explores the challenges to develop a policy model that can be applied to whole regions where terrorist groups procure arms and explosives, and discusses policy implications and actions that need to be taken in order to prevent such procurement. It is meant as a primer for experts, academics, and boots on the ground law enforcement officers to prevent organized as well as ad hoc acquisition of arms and explosives by terrorists.

Keywords: procurement, prevention, arms and explosives, IEDs, ISIS, Al-Qaeda, UN Sanction Committee 1267, proxy wars, porous borders, networks, terrorist financing, Turkey.
Terrorist organizations across the world have been responsible for more than 8,000 attacks in 2018, resulting in the deaths of 33,000 people and the wounding of nearly 23,000 others, according to the US State Department’s 2018 Statistical Annex Report.\(^1\) Although the overall number of terrorist attacks has decreased in recent years, the number of casualties resulting from specific attacks remains high largely because terrorist groups continue to use a wide variety of weapons. In 2018, firearms and explosives (e.g., dynamite, grenades, and improvised explosives devices or IEDs) were the most common types of weapons used by terrorist organizations. They also used vehicle borne improvised explosives devices (VBIED) and unmanned aerial vehicles (UAVs).\(^2\)

Terrorist groups in different regions of the world have the capacity to get access to a wide array of dangerous arms and explosives – from firearms, rocket-propelled grenades bombs, and IEDs to chemical weapons – and a few of them have even expressed a desire to lay their hands also on biological agents, radioactive devices, and chemical and nuclear weapons. Their ability to access and deploy conventional weapons in public places against unarmed civilians and in combat zones against unsuspecting soldiers makes terrorist tactics formidable. In some cases, terrorist weapons are technologically more sophisticated than those used by law enforcement and military.

A number of terrorist groups procure arms and explosives from rogue governments that support and sponsor terrorism. Additionally, endemic corruption, porous borders, weak law enforcement capacity, vast financial resources of some terrorist groups, and developed criminal networks have helped terrorist groups get access to arms and explosives on the black market. This chapter describes the arms and explosives terrorist groups have used, examines factors that allowed terrorist groups to access these arms and explosives, and recommends cogent policies for countering this trend.

## Arms and Explosives

There is great variety in the arms and explosives procured and used by terrorists. The US Department of State categorizes various weapon types in its global terrorism database, including fake weapons, incendiaries, melee weapons, vehicles, and sabotage equipment.\(^3\) “High range” weapons include biological agents, chemical weapons and radiological agents. “Medium range” weapons are automatic weapons, rocket launchers, and military-grade explosives. These are widely available from states sponsoring terrorism and on the international black market. “Low range” weapons include homemade weapons that can be manufactured from commercially available components. For instance, IEDs were used as roadside bombs against American forces in Iraq with lethal effects. IEDs can be homemade from ammonium nitrate and fuel oil (ANFO) - easily accessible materials.\(^4\) At the other end are sophisticated weapons of mass destruction which, except for some chemical weapons, are still beyond the reach of most terrorist groups.\(^5\)

One type of combat weapons are so-called “melee weapons”, varying from knives and machetes,\(^6\) to ropes or other strangling devices. Hands, feet, and fists also fall under the melee category.\(^7\) Melee weapons the primary group of weapons in the early history of terrorism. The Sicarii in antiquity and the Assassins in the Middle Ages had a preference for daggers to kill their targets.\(^8\) While melee weapons were do not have the visceral impact of an explosive device, they can easily be hidden and inflict serious bodily and psychological harm to their targets.\(^9\) Melee attacks have been more commonly seen in Africa and Latin America and lone actors continue to use melee weapons in Western European countries,\(^10\) and against Israel.\(^11\)

Firearms make up the second category of conventional weapons. The wide availability and short-range effectiveness of firearms account for their popularity among terrorist groups.\(^12\) Firearms include light and heavy infantry weapons and include assault rifles, machine guns, rocket-propelled grenades, mortars, and precision-guided munitions, but also, pistols, rifles and
submachine guns. Rifles use higher-powered ammunition than handguns, which makes the rifle useful in outdoor environments, thanks to its added length, power, and stability. Rifles can be semi-automatic, automatic, or single-shot. One of the most common type of rifles that terrorists prefer to use is the AK-47, or “Kalashnikov,” designed by the Soviet Union in 1946. With its minimal cost, ease of use and maintenance, and cheap, plentiful, powerful firing cartridge make the AK-47's one of the most preferred weapon among terrorists according to some authors. Similar to AK-47s, the American-made M-16 has been produced in large numbers and has been used by conventional as well as irregular forces.

Submachine guns are commonly used by the police and paramilitary services. Many older models are still accessible to terrorists on black and open markets. Shorter and lighter than rifles, terrorists appreciate their handling. The Precision-Guided Munitions (PGMs) use infrared or other targeting technologies and include the American Stinger, a shoulder-to-air missile. It was provided to Afghan mujahideen to target Soviet helicopters in the 1980s. It was an effective weapon, although it is not common to see PGMs in the hands of contemporary terrorists. Explosives comprise the third category of conventional weapons, and they are the category most frequently used by terrorist groups. In 2017, bombing was the most frequent category of attack by terrorist groups, as 47 percent of terrorist incidents recorded involved the use of explosives. Explosives can vary from crude homemade devices to advanced commercial or military-grade devices. Hand grenades are one of the simplest forms of explosives - they are easily portable with an effective range of at least five meters from the blast’s center. Its outer casing is designed to send out fast-moving projective metal fragments that maim and kill. Terrorists prefer to use hand grenades because they are easy and simple to carry, conceal, and to use.

Rocket-Propelled Grenades (RPGs) are uncomplicated but powerful explosives used by some terrorist groups to target bunkers and buildings. Terrorist groups who are capable of doing complex coordinated attacks often use RPGs in their operations. Hamas, the Taliban, and the Revolutionary Armed Forces of Colombia (FARC) are groups which commonly use RPGs. For example, Hamas fired over 4,000 RPGs and other rockets against Israeli targets in 2014 alone.

Bombs are one of the largest categories of the explosives. The vast majority of terrorist bombs are self-constructed and improvised weapons. Mines which are buried in the soil to be detonated as booby traps are also used. While terrorists use antipersonnel mines to kill their targets, anti-tank mines are designed to destroy entire vehicles. Terrorist groups in the Middle East, Asia, and Latin America which have used mines include the PKK in Turkey, the FARC and the National Liberation Army (ELN) in Colombia, and the Taliban in Afghanistan.

Improvised bombs are manufactured from commercially available explosives such as dynamite and trinitrotoluene (TNT). The invention of dynamite (made of nitroglycerin, sorbents, and stabilizers) in 1867 was one of the factors behind the rise of 19th century terrorism by anarchists and social-revolutionaries. It was first used by revolutionary groups in Russia and anarchists in Western Europe adhering to “the philosophy of the bomb.” Some of the compounds of 20th century terrorist bombs involved plastic explosives such as Semtex and Composite-4 (C-4), and ANFO explosives. The “shoe bomber,” Richard C. Reid, used plastic explosives in his attempt to target American Airlines’ Flight 63 by molding plastic explosives into his shoe. Semtex, a plastic explosive of Czech origin, is very common on the international market and large amounts of it were detected in Libya after the fall of Colonel Gaddafi in October 2011. The Irish Republican Army (IRA) was one of the groups who used Semtex obtained from Libya for its attacks in Northern Ireland and England. Like Semtex, C-4 is a powerful plastic explosive, based on nitroamine, developed originally by the US Armed Forces. It is not as easy as to obtain Semtex due to its high price. C-4s became accessible for terrorist groups after a rogue Central Intelligence Agency (CIA) agent had shipped 21 tons of
C-4 to Libya in the 1970s. Finally, ANFO explosives are developed when ammonium nitrate fertilizers are soaked in fuel oil. ANFO explosives have frequently been used for car or truck bombs, e.g., by the IRA in the UK and by the Tamil Tigers in Sri Lanka. Timothy McVeigh, a disgruntled American army veteran, used a two-ton ANFO explosive device, when he targeted the Alfred P. Murrah Federal Building in Oklahoma in 1995.25

Terrorist bombs vary from gasoline bombs, pipe bombs, and vehicular bombs to barometric bombs. Gasoline bombs, also called “Molotov cocktails,” are the most commonly used explosive weapon, manufactured by a gasoline-filled bottle with a burning cloth wick. Pipe bombs are easily formed and common types of explosives; they are filled with explosives and then capped on both ends. Pipe bombs have been used by single issue terrorists targeting abortion clinics in the US as well as in the 1996 Summer Olympics in Atlanta. Vehicular bombs wired with explosives are frequently used by terrorists. The fact that vehicular bombs are mobile and non-identifiable and capable of transporting large amounts of explosives make them appealing to terrorist groups. To date, a large number of terrorist groups have used such car and truck bombs in their attacks, including Peru’s Shining Path, the IRA, the Tamil Tigers, several Palestinian groups and the Basque Fatherland and Liberty (ETA).26

Homemade improvised rockets are also popular among terrorist groups, although they generally lack precision. Hamas and the Palestinian Islamic Jihad have used improvised rockets (dubbed Qassam) against Israel targets. Finally, barometric bombs are constructed with triggers that are activated by changes in atmospheric pressure. Such bombs have the capacity of blowing up an airliner in midair at a pre-set altitude, such as in the case of Pan Am Flight 103 en route from London to New York in December 1988, killing 259 people.27

Bombmakers use various types of explosives to construct more or less sophisticated triggering devices, enabling them to control timing and direction of the blast. Some examples of triggers are time switches, fuses, pressure triggers, electronic triggers, and high-technology triggers.28

Chemical weapons can have a serious impact, especially indoors while their lethality outdoors depends on wind and weather factors. When it comes to biological weapons, these are difficult to develop and control because of possibly longer infection paths and incubation times; but they can cause widespread and long-term mortality. Radiological devices have rarely been used and have mainly a psychological impact, but their casualty rates are low. Nuclear weapons (atomic and thermonuclear) are the most threatening type of WMD. So far, these have been beyond the reach of non-state terrorists.29

**Factors That Enable Terrorist Groups to Procure Arms and Explosives**

The 2017 Global Terrorism Database, produced by the National Consortium for the Study of Terrorism and Responses to Terrorism (START), located at the University of Maryland, listed more than 300 active terrorist groups in 2017. These represent a broad spectrum of ideologies, including tenets espoused by ethno-nationalist groups, left-wing groups, right-wing groups, as well as separatist and jihadist groups. Despite differences in their ideological leanings, all of these groups have one thing in common: the capability to procure arms and explosives to inflict harm in terrorist attacks. State-sponsored terrorism, endemic corruption, porous borders, financial capacity of terrorist groups, weak law enforcement, and the occasional convergence of criminal and terrorist networks all facilitate the ability of terrorist groups to acquire tools of destruction.
The Role of States in Sponsoring Terrorism

Acts of terrorism have been committed by single individuals, organized groups, and state-sponsored actors. Individually committed terrorist acts are often labeled “lone actor terrorism”; violent acts committed by militant organizations are labeled “group terrorism”; and violent acts committed by government agents may be listed as “state or regime terrorism.” State or regime terrorism has been defined as

“... an attack by a head of state and his law enforcement officers and the military on individuals, groups, political party opponents, or on other states, who are seen as threats to the government to deter others in the country and beyond from ever challenging its policies or messing with its vital interests.”

State terrorism can target political adversaries in the international domain or domestic enemies in the national domain. States taking a role in promoting terrorism provide ideological, financial, military, and operational support to perpetrators. A government’s military support includes supplying a broad range of weapons as well as military training, whereas operational support refers to the provision of false documents, special weapons, and safe havens. The US Department of State has created a detailed list of states that sponsor terrorism. It includes North Korea, Iran, Syria and (until recently) Sudan. Sudan supported regional terrorist groups throughout the Middle East and provided safe havens for the Al-Qaeda network, the Abu Nidal Organization, Hamas, and Hezbollah. Syria sponsored terrorist groups in particular in the Bekaa Valley in eastern Lebanon at least until 2005. Libya was another active country sponsoring terrorism in the 1980s and 1990s, providing training camps for many left-wing and jihadist groups. Iran actively sponsors terrorist groups in various parts of the world. Iran yearly spends $1 billion USD to sponsor terrorism. The Islamic Revolutionary Guards Corps (IRGC), which numbers some 125,000 personnel, was designated as a terrorist organization by the US in 2019. The IRGC continues to provide conventional weapons to a broad range of groups, including Hezbollah in Lebanon, Hamas in Gaza, the Palestinian Islamic Jihad, Kata’ib Hezbollah in Iraq and the al-Ashtar Brigades in Bahrain.

Proxy Wars

In the Cold War and beyond, states have used local proxies to defend or expand their interests abroad. The proxies can be local tribal militias or transnational terrorist groups or a combination of these. Currently, there has been such a proxy war between Iranian-backed and Saudi-backed groups in Syria and Yemen. In Syria, many foreign-supported jihadist groups mushroomed in different towns and provinces across the countryside since 2011, for example, the Hamza Division, the Sham Legion, the Syrian Front, Jash al-Nasr, and the Samarkand Brigade as well as Hay’at Tahrir al-Sham, Ahwar al-Sharqiya, Jaysh al-Izza, Hurras al-Din, and Ansar al-Tawhid. In Yemen, Al-Qaeda in the Arabian Peninsula (AQAP), Ansar Allah (Houthis), and ISIS’ Yemen branch have received, at one time or the other, foreign support. One of the procurement sources for arms and explosives for jihadist groups in Syria was governments which provided weapons to Syria’s belligerent groups. Saudi Arabia and the US provided weapons to allegedly “moderate” groups, but these weapons often changed hands. In some cases, arms and ammunition were looted from government forces in Iraq and Syria. In other cases, weapons were stolen from, or given away by members of moderate groups, who had been given weapons due to their resistance against Bashar al-Assad’s government. Turkey is another country that had strong links to jihadist groups targeting the Bashar al-Assad
government. For years, Turkey kept its border open for ISIS militants who traveled to Syria. A police investigation in 2014 proved the existence of arms and explosives transfers from Turkey to jihadist groups in Syria.

Conflict and post-conflict periods often create new opportunities for terrorist groups. For example, terrorist groups looted Iraqi military’s arms and explosives depots in 2003 when Saddam Husain was ousted. Some of these explosives were later used by ISIS and Hasd al-Shabi militias. Similarly, ISIS militants looted several Iraqi military weapon depots, containing tons of tank ammunitions, as well as anti-aircraft guns, mortars, shoulder-launched missiles, rockets, and mines. Similar looting on an even grander scale took place in Libya after the fall of Gaddafi in 2011.

**Porous Borders**

Porous borders enable terrorist groups and criminal organizations to move members, money, and equipment. Porous borders are those that cross treacherous terrain which is difficult to monitor, police, or govern. There are also undefined or new, ill-defined borders disregarding historical borders with people of the same ethnic or religious affiliation living on both sides. Both terrorist groups and criminal organizations can smuggle arms and explosives from one side to the other with few, if any, checkpoints standing in their way.

Terrorist groups in Africa enjoy the porosity of borders – borders drawn when European colonial powers carved up the African continent with little regard for ethnicity, religion, and local culture. The colonial powers aimed to create spheres of influence based on political and economic motives, thereby often creating artificial insecure and porous borders. Additionally, many borders in Africa lack effective administration and management. The lack of enforcement on Nigerian borders allowed Boko Haram to cross into neighboring Cameroon and Chad. The police seized a huge number of weapons including RPGs, rocket launchers, anti-craft missiles, and AK-47s smuggled from Libya and Mali to Nigeria’s Boko Haram. The porous border between Kenya and Somalia allows Al-Shabaab to target Kenya. In one incident in 2014, two Al-Shabaab affiliated guards bribed Kenyan border guards and transferred 50kgs of ammunition from Kenya to Somalia. Bangladesh is another example that shows how porous borders facilitate arms and explosives smuggling. Since 2016, the country recorded an upsurge of political violence by jihadist groups who procure weapons from across the India-Bangladeshi border. Produced in factories in India, weapons found their way to Bangladesh through the latter’s porous borders. Libya’s porous border with Chad and Niger is frequented by smugglers to transport arms and explosives.

The porous border between Turkey and Syria allowed the arrival of tens of thousands of foreign fighters with the Turkish government looking the other way for a long time. Most of ISIS militants traversed Turkey’s borders to travel to Syria. Turkey served as a base for the manufacture of improvised explosive devices used by ISIS. As a result, ISIS enjoyed Turkey’s neglect of its eastern borders.

One way terrorist groups smuggle arms and explosives is by tunneling under the borders. Nigeria’s police took some time to detect tunnels controlled by Boko Haram on its borders. Tunnels dug by Hamas were used to smuggle weapons from Egypt into Gaza. According to Israeli authorities, Hamas imported tons of explosives, fertilizers, and rocket-propelled grenades from Egypt via underground tunnels.

**Endemic Corruption**

Corruption in government creates operating spaces for terrorists. Terrorist groups capitalize on corruption by officials for avoiding controls while at the same time using claims of
corruption to legitimize their attacks against governments. Al-Qaeda leaders in particular were keen to use rampant corruption to motivate militants to target Muslim rulers.

Corruption is not only a facilitating factor for crime, but also for terrorism. According to one criminological theory, crime, corruption, and terrorism are entangled and can become inseparable.\textsuperscript{59} The list of some of the most corrupt countries overlaps with lists of countries with the highest number of terrorist incidents. For example, Somalia, Syria, Afghanistan, Iraq, and Yemen are among the top ten countries when it comes to terrorist incidents.\textsuperscript{60} and they also figure among the most politically corrupt countries.\textsuperscript{61} Terrorist groups in such countries find it sometimes easier to procure arms and explosives from corrupt customs and law enforcement officials and disloyal members of the military establishment.

**Links between, and Convergence of, Criminal and Terrorist Networks**

The convergence of criminal and terrorist networks creates a favorable environment for terrorist groups to access weapons. In a number of countries, criminal and terrorist groups are linked in various ways and they collaborate, sometimes on an ad hoc basis, sometimes permanently.\textsuperscript{62} Like terrorist organizations, many organized crime groups have evolved from top-down hierarchical organizations to loosely-connected functional units, often with a broad scope of activities, ranging from kidnapping to assassinations.\textsuperscript{63} Terrorist groups often network with each other. Similar to left-wing groups who collaborated and cooperated in the 1970s and 1980s in Latin America and Europe,\textsuperscript{64} jihadist groups from the Middle East have also networked with each other. Al-Qaeda-affiliated and ISIS-affiliated groups, while rivalling with each other, have cooperated at times in conflict zones in Syria. Investigations into the background of the Christchurch attack in New Zealand in 2019 unearthed evidence that right-wing extremist groups also network with each other. The Australian Brenton Tarrant traveled to Europe and attended training programs in Ukraine provided by the Azov Battalion.\textsuperscript{65}

The relationship between terrorist and criminal groups takes several forms, ranging from mere illegal business transactions as in arms sales, to alliances and even unification.\textsuperscript{66} Such alliances are based on sharing and exchanging expert knowledge on bomb making, money laundering, communication technologies, or operational support, such as access to smuggling tunnels and routes.\textsuperscript{67} Examples of this include Russian organized crime groups and the FARC trading weapons and cocaine, the IRA offering bomb-making expertise to the FARC and receiving financial assistance,\textsuperscript{68} and the Medellin cartel collaborating with the ELN to plant car bombs.\textsuperscript{69} Unification, while rare, can arguably be observed in the case of the Abu Sayyaf group, which sometimes had a political face and sometimes a more criminal appearance. Terrorist groups can degenerate into merely criminal groups. On the other hand, in some cases criminal groups develop political ambitions and their violence is not only based on profit motives. The situation gets even worse when rogue elements from government become part of such networks and when they ultimately manage to capture the machinery of the government itself.\textsuperscript{70}

**Financial Capacity of Terrorist Groups**

Terrorist groups are capable of buying arms and explosives due to various sources of income. A number of states were sponsoring guerrilla and terrorist groups abroad during the era of the Cold War. However, globalization and democratization trends accelerating during and after the 1990s have brought more accountability and transparency, making it riskier for governments to fund terrorist organizations. Nevertheless, there are still a number of states, including oil-
producing autocracies in the Middle East, sponsoring rebel groups engaging in terrorist tactics and providing them with arms or money to procure arms. Most terrorist groups use more than one method to procure funds for acquiring arms and explosives, including donations, taxation, extortion, and money earned from cross-border smuggling and trafficking. Some terrorist groups generate millions of dollars from criminal activities. Both the Colombian FARC and Peru’s Shining Path have been involved in drug trafficking, while Abu Sayyaf in the Philippines has generated revenues from kidnapping.

The IRA, operating in Northern Ireland, generated at one time $50 million USD in yearly revenues in donations from Irish Americans, while also profiting from dealing with electronics, oil, and cattle smuggling. Boko Haram in Nigeria reportedly made more than $50 million USD in revenue from kidnapping, bank robberies, and other illegal activities. Al-Shabaab, which seeks to overthrow the Somali government in order to form an Islamic caliphate, is said to earn more tens of millions of dollars a year from tolls and taxes.

The list of wealthiest terrorist organizations also features Laskar-e-Tayyiba, a Pakistani based terrorist group, that seeks to end Indian rule in the Kashmir region. Its reported $100-million USD revenue mostly comes from donations and, allegedly, also from contributions by Pakistan’s intelligence agency. Al-Qaeda, based in Pakistan and Afghanistan, is said to have $150 million USD in annual revenues, including from drug trafficking and ransom money from kidnappings. The Taliban is said to have a yearly $400 million USD in revenues, much of it from taxing opium farmers in Afghanistan. Lebanon’s Hezbollah is said to have a yearly annual budget of $500 million USD, half of which from the Iranian government and the rest from other donations and criminal activities like drug smuggling. Drugs are one of the main sources of income for the FARC which at one time was thought to be the source of half of the global cocaine supply. The Palestinian Hamas generated until recently much of its $1 billion USD budget from donations from Muslims abroad, the main donor being Qatar. The world’s richest terrorist organization is – or was – the Islamic State. ISIS was said to have a budget of around $2 billion USD in 2014 when it was controlling a huge swath of territory in Iraq and Syria. Reportedly, ISIS made $550 million USD from oil smuggling, and perhaps twice as much from looting banks in the towns it conquered, while also making between $20 and $45 million USD from kidnapping ransoms. In addition, revenue from antiquities sold on black and open markets was estimated to be around $36 million USD in 2014.

**Weak Law Enforcement**

One of the most effective counterterrorism strategies is to increase the capacity of law enforcement agencies. While law enforcement agencies are generally well-equipped and well-trained in developed countries in the Western world, and have the capacity to perform surveillance and wiretapping, and to deploy undercover agents and informants, their law enforcement counterparts among a number of countries in the developing world lack basic tools to fight terrorist groups, especially in rural areas. Weak state capacity has allowed the flourishing of criminal and terrorist groups in many parts of the world. For example, violence is all too common in Central America’s countries, ranking them among the top countries in homicide statistics. However, while most of the violence there is not political, it nevertheless affects the overall security situation.

Terrorist groups can more easily procure arms and explosives in states where law enforcement officials are not capable of enforcing the laws. The Afghan army and police have grave difficulty with fighting against well-trained Taliban militants. In some conflict zones, the government hires militia groups, such as the Civilian Joint Task Force in Nigeria, the Popular Mobilization Forces in Iraq, and the Rapid Support Forces in Sudan, to enforce the law and to fight terrorist organizations. However, such militia groups generally do poorly
against well-trained terrorist groups. Furthermore, such state-sponsored vigilante groups often violate both human rights and humanitarian law in their anti-terrorist missions.

Weak state capacity to fight against terrorist groups in sub-Saharan African countries led to the formation of international forces. ECOWAS, for example, consists of member states from the Lake Chad region and French forces, which fight against Boko Haram and Al-Qaeda affiliated groups in Mali. AMISOM consists of troops from four eastern African countries which fight against Al-Shabaab. In doing so, they have suffered from high casualties.

How Terrorist Groups Procure Arms and Explosives

In the following pages, the focus is on two types of terrorist groups, one secular, the other religious. The top ten terrorist groups, based on the number of terrorist incidents in 2017, include seven jihadist groups, two Maoist groups, and one separatist group. The jihadist groups were more violent than the Maoist groups. They procure arms and explosives using various tactics.

Jihadist Groups

Islamist organizations like ISIS, Taliban, Boko Haram, and Al-Shabaab are among the most violent terrorist groups in the world. Countries where these groups operate have recorded more than 60 percent of all deaths from terrorism in 2017. To kill so many people, they have developed a commensurate capacity to procure arms and explosives.

Al-Shabaab mainly uses firearms such as handguns, automatic weapons and rifles and explosives such as mortars, RPGs, IEDs, and landmines. Suicide bombing is frequently carried out by Al-Shabaab. Two of its primary sources of weapons are based in Yemen and Iran. In 2014, the Puntland administration in northern Somalia’s Bossaso port seized a boat carrying landmines and artillery shells, originating from Yemen. Another source of weapons for Al-Shabaab are African Union military bases, where the organization has seized weapons following successful attacks. For example, in 2016, Al-Shabaab attacked the El Adde military base where Kenyan troops were stationed, seizing assault rifles, machine guns, mortars, and rounds of ammunition. Al-Shabaab also seized weapons after it attacked Burundian and Ugandan military bases in Lower and Middle Shabelle. Furthermore, there have been reports indicating that Somali military personnel sell weapons and ammunition to Al-Shabaab.

ISIS has used basic assault weapons during many of its operations in Iraq. In addition, it uses IEDs, VBIEDs, suicide attacks, incendiary, and sabotage equipment. Houthis in Yemen are capable of using drones, ballistic missiles and boat-borne IEDs, with Iran said to be the main source providing arms and explosives to Houthis in Yemen.

Two widely acknowledged sources of arms and equipment for militant groups in Afghanistan are the black market and their disloyal elements from their enemies. Given the endemic corruption plaguing Afghanistan, these two often overlap. Corrupt officials have been alleged to sell weapons to militants, and the Taliban is also known for having been able to infiltrate Afghan security forces. Additionally, both ISIL-Khorasan and the Taliban often seize materials on the battlefield and during raids on government facilities. As a result, militants have been able to acquire night-vision goggles, high mobility multipurpose wheeled vehicles (Humvees), and other high-tech equipment.

Foreign support to the Taliban has also been reported. Russian agents have been accused of sending medium and heavy machine guns, small arms, and night-vision devices to the Taliban in recent years. Similarly, Iranian sources have been accused of supplying arms to anti-government forces in Afghanistan. To highlight such claims, American officials displayed Iranian-produced Fadjr rockets that had been confiscated from the Taliban at a public event in
November 2018. While it was noted that the markings and paint scheme show evidence of Iran origins, some political observers noted that the materials could have been purchased indirectly on the black market. Lastly, American officials, as well as many independent observers, have long stated that elements of Pakistan’s government provide material support to the Afghan Taliban.

In recent years, there have been reports of large transfers of rockets and other military equipment from Iran to Hezbollah in Lebanon. Some of these have reportedly been smuggled on land through tunnels and over water by small fishing boats to the Palestinian Islamic Jihad (PIJ) and Hamas. In 2014, Hamas attempted to use a Lebanon-based trading company to negotiate an arms deal involving missiles and communications equipment with North Korea.

Additionally, online marketplaces have provided a convenient source of dual-use military equipment. Palestinian militants have placed large orders with a China-based online marketplace for shooting gloves, tactical boots, small drones, laser sights, handheld radio equipment, knives, small motors, flashlights, and more. Rockets of varying types have been shipped to Palestinian terrorist groups, including GRAD rockets and laser-guided anti-tank missiles such as the Kornet, both manufactured in Russia; the M-302 long-range rocket manufactured by Syria and the FAJR-5 manufactured in Iran. Short-range mortars smuggled from Libya through Egypt are regularly used to strike border communities in Israel’s south.

Palestinian militant group members have also developed homemade weapons. The Al-Qassam Brigade, the armed wing of Hamas, developed its missile, appropriately names Qassam which is little more than a metal pipe packed with explosives with a 6-mile range, but lacking accuracy. Another locally manufactured missile is the M-75, a version of the Iranian Fajr 5 rocket with a 45-miles range. Palestinian militants also use the “Carlo,” a home-made submachine gun, often built with spare gun parts in small workshops throughout the West Bank. The Carlo has been used in several high-profile attacks.93

**Maoist Groups in India and the Philippines**

Maoist and communist groups operating in India and the Philippines are among the most active terrorist groups, based on the number of incidents.94 The New People’s Army have been conducting a protracted people’s war in the Philippines. Formed in 1969, the goals and strategies of the NPA closely aligned with Mao Zedong’s. In the 1970s, during China’s cultural revolution, the NPA sought support from Mao, who, in an effort to spread the communist ideology and China’s power, provided the group with weapons and funds from 1969 to 1976. With the conclusion of Mao’s Cultural Revolution, China’s government was stabilized and direct support for the NPA ceased. Without support from China, the NPA reportedly sought help from the Japanese Red Army (JRA), a Maoist faction of the Palestinian Liberation Organization (PLO), the Nicaraguan Sandinistas, as well as the Communist party of El Salvador.95

Today, without external support, the NPA primarily funds itself through imposing “revolutionary taxes” on the rural population and local businesses. In exchange for regular payment, the NPA refrains from attacking a business or farm. Others prefer to pay for this sort of Mafia-style “protection” in the form of small arms. While extortion activities pay for part of the NPA’s weaponry, most supplies are looted after ambushes on the Armed Forces of the Philippines (AFP), stolen from military vehicles, or purchased on the black market.96 Assault rifles like the Russian AK-47 and the American M-16 are relatively easy for the NPA to procure and maintain.

Militants of the Communist Party of India-Maoist (CPI, the Naxalites), are armed with cheap pistols, homemade weapons, and flintlocks. Naxalite arm-makers in the jungle are capable of making “Pahar” pellet guns and ammunition, as well as primitive rocket launchers. However, poorer members of the Naxalites are often armed with bows and arrows, axes, and
other primitive weapons. Better armed guerrilla squads, or “dalams,” each numbering up to 40 fighters are trained in special camps and sometimes even conduct dry runs before operations. They now possess US made submachine guns, Thomson guns as well as Russian and Chinese-made assault rifles.

Larger Naxalite units use, in addition to RPGs and rocket launchers, light machine guns, AK-47, L1A1 self-loading rifles, GF lightweight battle rifles, high-explosive hand grenades, and VHF radio sets to coordinate their attacks. The Naxalites have their own weapons manufacturing unit, the “Technical Research and Arms Manufacturing” (TRAM). The Naxalites frequently use IEDs and landmines against security forces in their areas of operation. Since a new CPI (Maoist) leader took over in November 2018, the use of explosives received renewed attention as the Naxalites started to use more sophisticated IEDs which can even be planted on trees. Explosive materials are acquired from mining areas. Though the majority of Naxalite weapons are captured or stolen from police and security forces – typically AK-47s, sometimes RPGs and heavy weapons – they also use underground arms market networks to purchase other, more sophisticated, weapons.

**Prevention of Arms and Explosives Acquisitions**

Effective counterterrorism models need to include strategies on how to prevent the procurement of arms and explosives by terrorist groups. There is an urgent need for many governments to make legislative and policy changes to ensure the implementation of preventive measures, strengthen the criminal justice response on the domestic front, and increase international cooperation and information exchange between states.  

**Upstream Prevention**

Upstream prevention includes macro-level strategies. According to Schmid, the pillars at this level of anti-terrorist prevention strategies encompasses good governance, democracy, rule of law and social justice. States sponsoring or enabling terrorism are actively providing arms and explosives to terrorist groups, despite the fact that the United Nations Security Council (UNSC) requires them to prevent weapons getting into the hands of terrorists. For example, the United Nations Security Council’s Al-Qaeda and Taliban Sanctions Committee 1267 asks member states to

“Prevent the direct or indirect supply, sale or transfer, to these [the listed] individuals, groups, undertakings and entities from their territories or by their nationals outside their territories, or using their flag vessels or aircraft, of arms and related materiel of all types including weapons and ammunition, military vehicles and equipment, paramilitary equipment…(…)…Member States are required to stop any supply or sale or transfer of arms and related material and services to listed individuals and entities…(…)…to prevent Al-Qaeda and other individuals, groups, undertakings and entities associated with it from obtaining, handling, storing, using or seeking access to all types of explosives, whether military, civilian or improvised explosives, as well as to raw materials and components that can be used to manufacture improvised explosive devices or unconventional weapons, including (but not limited to) chemical components, detonating cord, or poison….”  

97

98

99
Terrorists take advantage of porous borders in order to transfer arms and explosives from one country to another. Monitoring border areas surrounding conflict zones needs to be improved. Where states are weak, as is the case in some sub-Saharan countries, donors should provide local border guards, police with knowhow, equipment, and funding. UN conventions, protocols and Security Council resolutions on the prevention of arms transfers should be better implemented and continuously monitored by international observers.\textsuperscript{100}

\textit{Midstream Prevention}

Effective law enforcement models for fighting terrorism exist. These include curbing official corruption. In models where the element of countering corruption is missing, law enforcement has only limited success.\textsuperscript{101} A second element involves the fight against organized crime since that often involves smuggling and trafficking which, in turn, are linked to facilitating cross-border movements of terrorists. In several regions of the world, the fight against terrorist financing is failing. Furthermore, police and military need better training to detect the procurement of arms and control the theft of explosives. Additionally, regional cooperation among law enforcement agencies needs to be advanced, because terrorist groups operate across borders in networks. Finally, it is vital that governments support firearms identification, create effective record keeping of ownership of legal guns and rifles among members of society, and enhance control of storage facilities for explosives needed for legitimate purposes like road building in civil society.\textsuperscript{102}

\textit{Downstream Prevention}

Many law enforcement agencies and military units still lack modern training when it comes to combat terrorist groups. The law enforcement model of fighting terrorism and the military’s war model of fighting terrorism are difficult to integrate but it can be done as the British experience in Northern Ireland exemplified. Yet, further integration is needed, including the one between financial institutions and intelligence agencies. Since organized crime groups and terrorist groups often cooperate, government agencies tasked with fighting one for the other also need to cooperate better than traditionally. Domestic intelligence agencies and those dealing with foreign intelligence need to exchange information not only on an ad hoc basis but also as a daily routine. This should also go for international intelligence exchange. While this is already the case between many developed countries, there is still a long way to go in less developed parts of the world. In addition, embargoes should be imposed on states providing arms and explosives to terrorist groups. Banks which are found to enable money transfers between terrorist groups and arms dealers should be heavily fined if not shut down.

\textit{Conclusion}

Terrorist groups have been able to get access and use a variety of arms and explosives ranging from handguns, long rifles, submachine guns, incendiary, rocket artillery, mortars, and IEDs to grenades, VBIEDs, sabotage equipment, and unmanned aerial vehicles. Terrorist groups have commonly used firearms or explosives in their attacks, whereas a small percentage of terrorist incidents recorded the use of both in the same attacks.\textsuperscript{103} They have different sources to acquire arms and explosives. A greater part is due to spill-overs from the legal arms industry and military markets into illegal channels. Despite standard denials, it is clear that regular arms dealers and governments sponsoring militant groups abroad provide a large part of the weapons and explosives. Libya, Pakistan, Syria, and Iran are among the countries which reportedly
supported armed groups abroad, some of which have been involved in acts of terrorism in the past.\textsuperscript{104}

Terrorist groups take advantage of inter-state rivalries and, in turn, are used by state actors. They also take advantage of badly policed borders, corrupt government officials and weak law enforcement capacity on the national level and insufficient or lacking regional law enforcement cooperation. Furthermore, organized crime groups operating black markets enable terrorist groups to procure weapons.

Against this background, it is difficult to prevent the procurement of arms and explosives by terrorist groups. However, counter arms procurement strategies can reduce terrorist groups’ access to weapons and explosives, as long as they include effective policies in the areas of preventive and security measures, criminal justice response, and international cooperation. More specifically, the international community needs to strengthen its cooperation and continue engaging national institutions. There is a need to do policy analysis and develop models on how terrorists obtain weapons on the dark web. It is imperative to encourage postal agencies to flag suspicious packages, considering the fact that terrorist groups increasingly use mailing systems to transfer weapons. States need to share best practices to prosecute arms traffickers. Tracing of weapons still remains a challenge for many states. The governments need to prioritize their preventive measures against the diversion of weapons from government stockpiles to terrorist groups. States need to develop tracing technologies and conduct investigations to determine where illicit weapons originate. These are several recommendations for national institutions and the international community. The world urgently needs effective measures to prevent the procurement of arms and explosives by terrorists. Otherwise, global terrorism databases will continue recording thousands of casualties each year.

\textit{Mahmut Cengiz is Assistant Professor and Research Faculty member with the Terrorism, Transnational Crime and Corruption Center (TraCCC) at the Schar School of Policy and Government of George Mason University. He has international field experience, delivering capacity building and training assistance to international partners in the Middle East, Asia and Europe. He also worked on various research projects for the Brookings Institute, the European Union, and for U.S. government agencies. Mahmut Cengiz regularly publishes books, articles and op-eds on the Syrian conflict, terrorism, transnational crime, and corruption in the Middle East. His book, “The Illicit Economy in Turkey: How Criminals, Terrorists, and the Syrian Conflict Fuel Underground Economies” (2019), analyzes the role of criminals, money launderers, and corrupt politicians and discusses the involvement of ISIS and al-Qaeda-affiliated groups in underground economies. Mahmut Cengiz holds two Masters and two doctorate degrees. His graduate degrees in sociology were obtained at Turkish universities. He holds a Master’s from the American University School of International Service Program and a doctorate from the School of Public Policy program at George Mason University. Currently, he teaches Terrorism, American Security Policy and Narco-terrorism courses at George Mason University.}
Endnotes

3 Global Terrorism Database, Global Terrorism Database Codebook,’ START (University of Maryland), July 2018, pp. 28-29. Available at: https://www.start.umd.edu/gtd/downloads/Codebook.pdf.
6 Ibid., p. 58.
9 Casserleigh and Merrick 2013, p. 58.
12 Casserleigh Merrick 2013, p. 58.
13 Martin 2018, p. 10, p. 133.
15 Martin 2018, p. 266.
16 Ibid., p. 265.
17 Martin 2018, p. 266.
19 Casserleigh and Merrick 2013, p. 60.
21 Israel Ministry of Foreign Affairs, ‘Rocket fire from Gaza and ceasefire violations after Operation Cast lead,’ Israel Ministry of Foreign Affairs. Available at: https://mfa.gov.il/MFA/ForeignPolicy/Terrorism/Pages/Palestinian_ceasefire_violations_since_end_Operation_Cast_Lead.aspx.
22 Martin 2018, p. 266.
23 Ibid., p. 267.
26 Martin 2018, p. 268.
27 Ibid., p. 269.
28 Ibid., p. 267.
29 Casserleigh and Merrick 2013, p. 65.

31 States’ involvement in terrorism is explained by either the “patronage model” or the “assistance model.” While the “patronage model” means the active involvement of states in repression, violence, and terrorism through its agencies and personnel, the “assistance model” refers to tacit participation in terrorism with the assistance of sympathetic proxies and agents. States can have three different roles when involved in terrorism: as “sponsor,” “enabler,” or “cooperator.” First, the “sponsor” actively promotes terrorism, which is called state-sponsored terrorism. Second, the “enabler” refers to a state which enables terrorist acts to occur. Third, the “cooperator” refers to a state which fails to collaborate with other states in countering terrorism. Martin 2018, p. 72 and p. 75.

32 Ebbe 2016, p. 47.

33 Ibid., p. 71.

34 Ibid., p. 79.

35 US Department of State, ‘State Sponsors of Terrorism,’ Bureau of Counterterrorism. Available at: https://www.state.gov/state-sponsors-of-terrorism/.


39 Ibid.


45 Based on a tip-off, the military police frisked two trucks on the way to Syria and found some arms and explosives hidden beneath the humanitarian aid. Despite the obstacles to shut down this investigation, the media was able to publish the video footage showing the arms in the truck. Later investigation revealed that those arms were to be provided to an Al-Qaeda affiliated group in northern Syria. Additionally, the police recorded another incident in 2012, when it seized some materials used to manufacture chemical weapons. The government attempted to shut down this incident, releasing the Syrian criminals. However, it was found that the Syrian criminals attempted to transfer chemical materials to jihadist groups in Syria.


Onuoha 2013.


Ibid.


Some examples for intra-networking between criminal groups would be how Nigerian cocaine traffickers transferred drugs from Turkey to China, hiring Uzbek and Azeri couriers and networking between Turkish and Chinese drug trafficking groups. In another case, Turkish, Bulgarian, and Iranian criminal groups cooperated to transfer heroin from Iran to Spain, hiring a Malaysian courier. Cengiz, Mahmut, Turkish Organized Crime from Local to Global. Germany: Riga: VDM Publishing, 2011 p. 26, p. 28.


Ibid.

Ibid.

Ibid.


One of the notable attacks by the group was a series of bombings and shootings, carried out across Mumbai, resulting in the death of 166 people and injuring over 600 people.

Zehorai 2018

Ibid.

Ibid.

Ibid.


Bamidele, Oluwaseun, ‘Civilian Joint Task Force (CJTF) – A Community Security Option: A Comprehensive and Proactive Approach of Reducing Terrorism,’ Journal for DERADICALIZATION, 7, summer 2016, pp. 124-144. Available at:https://journals.sfu.ca/jd/index.php/jd/search/authors/view?firstName=Oluwaseun&middleName=&lastName=Bamidele&affiliation=&country=


Kurdistan Workers’ Party (PKK) conducted 159 attacks in 2017. See ibid.

For example, the number of total deaths was 206 in 295 attacks perpetrated by Maoist groups, whereas it was 1287 in 276 attacks conducted by Boko Haram in 2017. See ibid; United States State Department, ‘Annex of Statistical Information, Country Reports on

88 Ibid.


96 Ibid.


100 Ibid.

101 The Turkish police was considered as one of the most developed and successful police organizations in the region until corruption scandals implicating the government itself surfaced in December 2013. Then the government retaliated by purging all anti-terrorist units, thereby deleting institutional memory accumulated over the last decades. Turkish law enforcement largely failed to fight corruption. Cf. Cengiz, Mahmut and Mitchel P. Roth, The Illicit Economy in Turkey. Lexington: University of Maryland, 2019.


Bibliography


Israel Ministry of Foreign Affairs, ‘Rocket fire from Gaza and ceasefire violations after Operation Cast lead,’ Israeli Ministry of Foreign Affairs. Available at: https://mfa.gov.il/MFA/ForeignPolicy/Terrorism/Pages/Palestinian_ceasefire_violations_since_end_Operation_Cast_Lead.aspx.


DOI: http://dx.doi.org/10.19165/2018.1.06.


United States Department of State, ‘State Sponsors of Terrorism,’ Bureau of Counterterrorism. Available at: https://www.state.gov/state-sponsors-of-terrorism/.


Web Sources


Transparency International, ‘Corruption Perception Index 2018’ Transparency International. Available at: https://www.transparency.org/cpi2018
Chapter 17

Prevention of CBRN Materials and Substances Getting into the Hands of Terrorists

Ioannis Galatas

Chemical, Biological, Radiological and Nuclear (CBRN) threats are ranked very high on the list of near future threats due to their expected extraordinary impact on societies affected. After the 9/11 attacks that raised the terrorism concerns to a new level, many security experts believed that a CBRN attack was only a matter of time (“when, not if”). The fact that the world has not experienced a major CBRN incident from non-state actors since then does not mean that terrorists are not pursuing the acquisition of hazardous materials, namely chemical weapons, biological agents or nuclear and radiological materials to be deployed with or without the use of explosives. Therefore, it is imperative to prevent CBRN materials and substances getting into terrorists’ hands. In order to do this, we need to explore and map all the sources and pathways for terrorists to achieve their goals, so we can better provide assistance, guidance, support, and technical expertise to relevant actors. This chapter will focus on prevention and will try to uncover existing gaps, thereby facilitating possible solutions and develop countermeasures that will lead to better control of CBRN agents and a more efficient management of a very serious (near) future problem.

Keywords: CBRN, materials, substances, agents, dirty bomb, terrorists, smuggling, biological, chemical, radiological, nuclear, Al-Qaeda, ISIS
The modern world faces a number of conventional (natural or man-made) and non-conventional (including asymmetric) threats that range from natural disasters to urban bombings, including the accidental or intentional release of chemical, biological, radiological, or nuclear materials (CBRN), without or with the aid of explosives (CBRNE). Who could be behind some of these threats? Could it be states, terrorist organization or even lone actors?

Two recent developments in particular, have alarmed security agencies worldwide – jihadi plots disrupted before chemical and biological agents were used in a terrorist attack. In the first incident (July 2017) a plot involving a chemical improvised device able to release hydrogen sulfide was discovered in time in Sydney, Australia.¹ A second incident, uncovered in 2018, saw a Tunisian national being prevented from using ricin (84.3 milligrams were confiscated), a highly dangerous biological toxin found in his apartment.²

Although CBRNE is synonymous with weapons of mass destruction, the term “destruction” is appropriate in a strict physical sense only to the nuclear element (N) and its potential. Chemical weapons (C), certain Category “B” (biological) agents and radiological (R) dispersal (dirty bombs) or emitting devices might cause “disruption” rather than destruction when released. Destructive impact depends also on the size of the target: attacking a small village can be totally destructive while a same size attack in a major city with a population of 10 million or more would, relatively speaking, not be “destructive” to the same extent. In addition, the magnitude of destruction cannot be defined by the numbers of casualties. It should also be noted that CNE threats represent acute emergencies, while a bioterrorism attack or a pandemic are gradually developing emergencies that depend on the incubation period of the pathogen, its virulence, toxicity, and related factors.

The complexity and unpredictability of these threats are high. At the moment, many potential CBRN events are of low probability but of potentially very high impact.³ This is why political leaders are reluctant to take pre-emptive measures; these can have a substantial price tag and there are so many possible targets from critical infrastructures to mass gatherings. Unfortunately, many people forget that the unexpected can happen. The ongoing Covid-19 pandemic is evidence of this.

In addition, the feasibility of CBRN attacks is directly linked to the high number of potential targets. Soft targets, of which there are too many, are, by definition, not prepared to handle a CBRN incident. Therefore, the only viable solution is to invest in prevention measures in an effort to keep CBRN materials and substances out of reach for terrorists. Unfortunately, this is not an easy task to perform; it requires in-depth knowledge of the agents involved, the pathways used in their production and possible acquisition and, most important of all, continuous global exchange of information, since all countries face the same threat, even if some are thought to be preferred targets.

**CBRN Materials and Substances**

*Chemical Weapons*

Under the chemical weapons’ roof there are original chemical warfare agents, dual use chemicals or precursors, toxic industrial chemicals and the equipment/munitions to be used for the dispersal of these agents both in open fields and in urban environments. Toxic chemical agents are gaseous, liquid, or solid chemical substances causing death or severe harm. Chemical weapons include blister agents, nerve agents, choking agents, and blood agents, as well as non-lethal incapacitating agents and riot-control agents when deliberately used to harm people. Chemical weapons are categorized as:

1. nerve agents like sarin, soman, tabun or VX affecting mainly the nervous system;
2. blister agents (i.e., mustards), mainly affecting the skin;
3. pulmonary agents like phosgene or chlorine damaging the lungs;
4. blood agents like cyanide affecting the oxygenation of the body;  
5. tearing and incapacitating agents like mace, CS, CR, or capsaicin used mainly in riot control operations; and  
6. psych/mood modifying agents like LSD.

**Biological Weapons**

Biological weapons are warfare agents that directly or indirectly intentionally affect humans, animals or vegetation. These agents can be disseminated by spraying or by mixing with food/water and can involve viruses, bacteria, prions, toxins or fungi. Biological agents such as these as well as toxins can be turned into weapons delivered in the form of liquid droplets, aerosols, or dry powders. Currently, scientists are concerned that a modern technique called Clustered, Regularly Interspaced, Short Palindromic Repeat (CRISPR) is becoming more widely available, allowing even amateurs to start experimenting. The technique works like genetic scissors, allowing to cut away existing DNA code and replace it with new ones. This new technique is now available in the market place where anybody can buy certain do-it-yourself kits that might cause big problems to public health authorities (e.g., E. coli resistant to antibiotics kits are already for sale on the internet for under £ 100). On the other hand, terrorists with a scientific background or rogue scientists supported by cyber-criminals, might be able to genetically interfere in the genetic code of existing pathogens and transform them into more malicious agents affecting both humans and animals.

While the capabilities of organizations like Al-Qaeda have so far not matched their ambitions, there is little doubt about their motivation to use them chemical and biological weapons. Al-Qaeda’s spokesman Abu Gheith stated in 2002:

“We have the right to kill four million Americans, two million of them children … and cripple them in the hundreds of thousands. Furthermore, it is our obligation to fight them with chemical and biological weapons, to afflict them with the fatal woes that have afflicted Muslims because of their chemical and biological weapons.”

**Radiological Weapons**

Commonly known as “dirty bombs,” these weapons use conventional high or low explosives for dispersal as well as other means to spread radioactive material which may lead to short- and long-term health problems of the affected population and cause extended territorial radioactive surface contamination. Radiological weapons do not require nuclear weapon-grade materials; only some radioactive substance of sufficient potency to achieve harmful effects. There are four types of radiological dispersion.

First, a radiological dispersal device (RDD) in the form of a conventional explosive attached to radioactive material (“dirty bomb”). RDD consequences include loss of lives (more from the explosion than the radioactive pollution) psychological shock, business disruption and high decontamination costs. Second, is a silent release of radioactive materials in the air, the water, or on the soil by aerosol, dilution or dusting. Third, is a stationary radiological emission at a place where people reside (Radiological Emission Device – RED: e.g., an uncapped lead container left under the seat of a metro train). Fourth, is an attack on a storage site of radioactive materials resulting in subsequent dispersal – i.e., a waste storage facility or a hospital or the hospital’s blood bank using a cesium irradiator.

Some of the most dangerous radioisotopes are: Cobalt-60, Americium-241, Cesium-137, Iridium-192, Plutonium-239 and 238, Strontium-90, Californium-252, Radium-226, and Lead-
The half-life of certain radioisotopes is of security concern, such as: Americium-241 (433 years); Californium-252 (2.7 years); Cesium-137 (30 years); Cobalt-60 (5.3 years); Iodine-131 (8.0 days); Iridium-192 (74 days); Polonium-210 (140 days); Plutonium-238 (88 years); Plutonium-239 (24,000 years); Radium-226 (1,600 years); and Strontium-90 (29 years).

**Nuclear Weapons**

While there are different types of nuclear weapons, all employ nuclear fission or fusion reaction for unfolding their explosive power. Most nuclear weapons today are two-stage thermonuclear weapons that derive their explosive energy from the combined power of nuclear fission and fusion. That is, an initial fission reaction generates high temperatures needed to trigger a secondary – and much more powerful – fusion reaction, hence the term “thermonuclear.” Sufficient quantities are required in order to construct an atomic bomb such as Plutonium (Pu-239) – 7-8 kg; Plutonium Oxides (PuO₂) – 10 kg; Metallic Uranium (U-235) – 25 kg; Highly Enriched Uranium Oxide (UO₂) – 35 kg; Intermediately Enriched Uranium Oxides – around 200 kg. In April 2004, Abu Mus’ab al-Zarqawi, former leader of Al Qaeda in Iraq, stated “If we had such a nuclear bomb – and we ask God that we have such a bomb soon – we would not hesitate for a moment to strike Israeli towns, such as Eilat, Tel Aviv, and others.”

Critical nuclear materials are distributed mainly in one of the ten countries possessing nuclear weapons such as Russia, the US, France, UK and China (~99% of highly enriched uranium) while a small proportion (1%) is spread among 40 countries (including India, Pakistan, North Korea and Israel), in about 100 sites worldwide – in over 130, often ill-protected, research reactors. In addition, there are 250 metrics tons of separated plutonium in military stockpiles and 250 metric tons in civilian stocks, held mostly in Russia, the US, France, Germany, the UK; some in Belgium, China, India, Israel, Japan, North Korea, Pakistan, and Switzerland.

Two nuclear specialists estimated that, for $2 million, a terrorist group could acquire the necessary equipment, personnel, non-fissile material, and transportation support to build a crude nuclear device. For an additional $8 million, they speculated that enough bomb-grade material could be acquired. It is by no means beyond the realm of possibility that a terrorist group of reasonable size would leverage such resources for a nuclear project. Modern terrorist movements like Aum Shinrikyo in the 1990s and later on al Qaeda and ISIS (even after the defeat suffered), had or could have this level of resources at their disposal. On the other hand, it has to be noted that of the 31 countries who at one time were considered developing nuclear weapons, only ten produced a deliverable atomic bomb. Seven countries with a formal nuclear weapons program gave up their attempts.

**Explosives**

An improvised explosive device (IED) is a type of unconventional explosive weapon that can take any form and be activated in a variety of ways. They target soldiers and civilians alike. In the second Iraq War, IEDs were used extensively against US-led invasion forces and by the end of 2007 they had become responsible for approximately 63% of coalition deaths in Iraq. They are also used in Afghanistan by insurgent groups. In 2009 alone, there were 7,228 improvised explosive device (IED) attacks in Afghanistan, a 120% increase over 2008, and a record for the war. IEDs can be used to disseminate C/R agents. IEDs cannot be combined with biological agents since the heat produced during detonation might kill most of the pathogens. Weaponized biological warfare agents follow a complex methodology of dispersal sustaining the survivability of the organisms.
Concerns and Vulnerabilities

The situation in certain parts of the world generates concerns and elicit vulnerabilities. In a 1999 article, Alex Schmid noted that some of the conflict zones (e.g., in the Caucasus) host civic nuclear facilities or research institutes that could be used for theft or fabrication of WMD while the civilian nuclear industry produces huge amounts of plutonium which is attractive to thieves. In addition to rogue scientists, organized crime might become involved in the procurement and transport of nuclear materials since concealment and transport of some of these weapons are, due to their small size, relatively easy. On top of the above, urbanization has increased the chance of mass fatalities in the case of an attack.\(^{14}\)

In the international literature, there are many scenarios exploring a biological or chemical attack eliciting mass casualties. For example, there is the popular scenario of a small airplane (e.g., a crop sprayer) flying over a metropolitan city spraying 50 to 100 kg of anthrax spores, with the potential of killing from 130,000 to 3,000,000 citizens, depending the meteorological conditions.\(^{15}\) This scenario and a few others are still far beyond the capabilities of modern terrorists even if they have the scientific background to culture \textit{B. anthracis} and create a collection of spores.\(^{16}\) This scenario is more indicative of a rogue state attack against another country and might result in severe retaliation – e.g., in the form of a nuclear attack.

But the same scenarios can be seriously considered on a much smaller scale focusing on specific targets (i.e., the staff of an embassy) or be used for assassination purposes (e.g., the North Korean VX attack in a Malaysian airport; ricin letters mailed to US officials, etc.). Despite the widespread perception assuming that terrorists are pursuing the acquisition of CBRN agents, a more realistic assessment makes clear that there are certain inhibiting factors that should make even terrorists reluctant to be using weapons of mass destruction even if they may be able to lay their hand on them. In general, there is a:

1. general reluctance to experiment with unfamiliar weapons;
2. lack of familiar precedents;
3. fear that the weapon would harm the producer (i.e., radiation) or user;
4. fear of alienating relevant constituencies and potential supporters on moral grounds;
5. fear of unprecedented governmental crackdown and retaliation targeting them, their constituencies or sponsor states;
6. lack of a perceived need for indiscriminate, high-casualty attacks for furthering goals of the group; and
7. lack of money to buy nuclear material on the black market.\(^{17}\)

The latter might not be the case, during the period that ISIS was thriving and a significant amount of financial resource was available from a spectrum of sources (e.g., oil smuggling, extortions, kidnapping for ransom, robberies, etc.). It is of note that the 40kg of low-grade uranium stolen from the University of Mosul, Iraq (2014), is still missing. That material is not good enough for assembling a nuclear bomb, but might be used for a radiological dispersal device.\(^{18}\)

Dual-Use Items of Proliferation Concern

Dual-use goods and technologies refer to those that are capable of, or were designed for, use for peaceful and legitimate civilian or commercial purposes, but also have potential applicability in the development or enhancement of weapons’ programs, including WMDs. Dual-use refers not only to certain chemicals (e.g., dimethyl methyl phosphonate, thiodiglycol or arsenic trichloride), but also to certain biological agents with a bioterrorism potential.
The Chemical Weapons Convention requires declarations about, and inspections of, industrial facilities that produce, process or consume more than specified threshold amounts of certain chemicals, dual-use and otherwise. Specific requirements and procedures vary, depending on the risk a chemical substance poses to the object and purpose of the Convention. Based on the degree of this risk and the extent of their commercial application, chemicals are divided into three so-called Schedules, which form an integral part of the Convention. Each of the three Schedules contains lists of toxic chemicals and precursors with corresponding Chemical Abstracts Service (CAS) registry numbers. The Organization for the Prohibition of Chemical Weapons (OPCW) in The Hague maintains a database of approximately 32,000 scheduled chemicals on its website, a small portion of all possible scheduled chemicals. Riot control agents (RCAs), such as tear gas and pepper spray, are not included in any Schedule.

**Who is Interested in the Malicious Use of CBRN Agents?**

Apart from the military use of CBRN agents by rogue regimes (officially forbidden; the majority of chemical and biological weapons have been destroyed under relevant conventions), terrorists are the second group interested in their acquisition and possible use against soft targets around the globe.

**Al Qaeda**

In the period before 9/11, al Qaeda made several unsuccessful attempts to obtain radiological and nuclear materials. Despite these failed efforts to acquire the appropriate materials, technology and know-how, Osama bin Laden, stated: “Acquiring chemical and nuclear weapons for the defense of Muslims is a religious duty.” (…) Adding: “It is the duty of Muslims to prepare as much force as possible to terrorize the enemies of God.” In the same vein, Abu Mus’ab al-Suri stated:

“…. we are serious about acquiring all possible weapons and means and will deal with you the same way, in accordance with our true religion. (…) Hitting the US with WMD was and is still very complicated. Yet it is possible after all, with Allah’s help, and more important than being possible – it is vital.”

Al-Suri further stated, “…. if those engaged in jihad establish that the evil of the infidels can be repelled only by attacking them with weapons of mass destruction, they may be used even if they annihilate all the infidels.”

**ISIS**

In June 2014, Jama’at al-Tawhid wal-Jihad, a group which previously had pledged allegiance to al-Qaeda, proclaimed itself as a worldwide caliphate and began referring to itself as the ‘Islamic State’, claiming religious, political and military authority over all Muslims worldwide. The atrocities conducted by this group were beyond the pale of conventional ethics. It was also the first time that terrorists used chemical weapons against their opponents in both Syria and Iraq.

**European Jihadists Returning from Syria and Iraq**

Since the Syrian conflict began in 2011, thousands of EU nationals and residents have traveled,
or attempted to travel, to conflict zones in Iraq and Syria to join insurgent terrorist groups, such as ISIS. Research conducted in 2016 estimated that the contingent of foreign fighters originating from EU Member States (mostly from Belgium, France, Germany, and the UK) numbered between 3,922 and 4,294 individuals. Of those, it has been estimated that around 30% had already returned to their home countries by 2016.²⁵

Returning jihadists are perceived as a security threat mainly because they have real combat experience and can serve as role models for radicalizing new recruits, raise money for terrorism or even conduct retaliation attacks against targets in their homelands.²⁶

A number of returnees have academic and/or professional backgrounds relevant to the science behind CBRN threats. Apart from the real combat experience that they might have gained, some might have been recruited in the inner nucleus of those involved in handling or producing chemical weapons that subsequently were released on the battlefields of Syria and Northern Iraq. Alternatively, they might have been involved in the safe and secret storage for future use of the radioactive material stolen from the University of Mosul in Iraq or they might have been employed in the mass production ammunition and explosives (IEDs) factories operating in the territories under ISIS control until late 2018.

After losing the war on all fronts in Syria and Iraq, most of these European jihadists found themselves to be deprived of a homeland, with limited resources, wanted by local and international coalition forces, and facing the dilemma either to return back to Europe or migrate to another relatively “safe” conflict theatre like the Philippines, Indonesia, Yemen or Afghanistan, etc. The current, “second generation,” whose departures were interlinked with the activities of ISIS, is perceived to be “more battle-hardened and ideologically committed,” and may have come back with violent motives including to harm EU citizens. Due to their loss of territory, many of them feel angry and some of them may harbor a strong desire to do harm to as many people they are capable of hurting by using their destructive know-how attained abroad. Although most of them are already known to national authorities and are under surveillance they are aware that most states do not have the resources and manpower to follow them 24/7 or to record all their contacts via the social media and dark web.

Various other Actors

After 9/11, a number of CBRN-related plans and plots have been uncovered, including these:

- a plan by US citizen José Padilla (2002: dirty bomb attack in the US);
- the Benchellai’s “Chechen Plot” in France (2002) against Russian interests in Europe, involving C or B (probably Ricin);
- the 2003 Bourgass’ Ricin poison plot (by using castor beans in London);
- the plot by Indian-born British Dhiren Barot (2004: constructing dirty bombs from smoke detectors containing Americium-241 targeting the New York Stock Exchange, IMF headquarters, and the World Bank by using limousines packed with explosives and radioactive “dirty” bombs);
- the 2007 Iraq attacks with vehicle-borne explosives (VBIEDs) and chlorine gas containers;
- the 2018 Cologne plot orchestrated by the Tunisian Sief Allah H. who was manufacturing an explosive device which incorporated the highly toxic substance Ricin.²⁷

There are several cases of CBRN-based attacks that have been carried out or attempted by secular groups. For example, in 1990 the Tamil Tigers (LTTE) stole drums of chlorine gas from a chemical facility and then used these against the Sri Lankan army.²⁸ There is one important thing that must be understood when it comes to CBRN terrorism. Among the hundreds of violent non-state actors that populate the field of terrorism, only a small percentage
of these are actually willing – for a variety of reasons – to resort to CBRN terrorism. Within this smaller subset of willing groups, an even smaller percentage has the capability to engage in CBRN activities. The difficulties inherent in such an endeavor are well summarized in the experience of the Japanese apocalyptic cult Aum Shinrikyo.\textsuperscript{29} Despite its vast resources, expertise, and – as a religious cult – de facto immunity from government interference – Aum fell short of expectation, as the group’s sarin gas assault in the Tokyo subway was not able to achieve the level of destruction desired. Identifying those groups that possess both the motivation and the capability is a first step in thwarting the CBRN threat.\textsuperscript{30} A number of mechanisms exist which can contribute to fight the proliferation of CBRN technologies.

**International Regulation and Control Bodies**

There are a number of international instruments meant to control CBRN materials and uses. However, most of these refer to state actors and their proliferation concerns with regard to other state actors.

**Treaties and Conventions**

There are several important treaties and conventions:

- Nuclear Non-proliferation Treaty (NPT):\textsuperscript{31} Prevents the spread of nuclear weapons and weapons technology, to promote cooperation in the peaceful uses of nuclear energy and to further the goal of achieving nuclear disarmament and general and complete disarmament.
- Biological and Toxins Weapons Convention (BWTC):\textsuperscript{32} Effectively prohibits the development, production, acquisition, transfer, retention, stockpiling and use of biological and toxin weapons. The convention is a key element in the international community’s efforts to address the proliferation of weapons of mass destruction.
- Chemical Weapons Convention (CWC):\textsuperscript{33} Aims to eliminate an entire category of weapons of mass destruction by prohibiting the development, production, acquisition, stockpiling, retention, transfer or use of chemical weapons by States Parties.
- Hague Code of Conduct Against Ballistic Missile Proliferation (HCOC):\textsuperscript{34} This code of conduct is the result of efforts of the international community to internationally regulate the deployment of ballistic missiles capable of carrying weapons of mass destruction.

**Export Control Regime**

There are also several important export control regimes:

- The Nuclear Suppliers Group (NSG)/Zangger Committee:\textsuperscript{35} This is a group of nuclear supplier countries that seeks to contribute to the non-proliferation of nuclear weapons through the implementation of two sets of Guidelines for nuclear exports and nuclear-related exports.
- The Australia Group (AG):\textsuperscript{36} An informal forum of countries which, through the harmonization of export controls, seeks to ensure that exports do not contribute to the development of chemical or biological weapons.
- The Wassenaar Arrangement:\textsuperscript{37} This mechanism has been established in order to contribute to regional and international security and stability, by promoting
transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thereby preventing destabilizing accumulations of arms.

- The Missile Technology Control Regime (MTCR):\textsuperscript{38} restricts the proliferation of missiles, complete rocket systems, unmanned airborne vehicles, and related technology for those systems capable of carrying a 500 kg payload at least 300 km, as well as systems intended for the delivery of weapons of mass destruction (WMD).

### Emerging Technologies

Technical innovations can weaken control over the illicit use of CBRN agents and materials, but at the same time they can also assist in the prevention of CBRN attacks.

#### Drones

A drone, in technological terms, is an unmanned aircraft. Drones are more formally known as unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UASs). Essentially, a drone is a flying robot that can be remotely controlled or fly autonomously through software-controlled flight plans in their embedded systems, working in conjunction with onboard sensors and GPS.\textsuperscript{39} Drone swarms consist of multiple unmanned platforms and/or weapons deployed to accomplish a shared objective, the platforms and/or weapons autonomously altering their behavior based on communication with one another or with a ground pilot approving (for the time being) firing decisions. The interconnectivity of drone swarms enables them to exhibit more complex behaviors than their component drones. There is a significant distinction between drone swarms and drones \textit{en masse}.\textsuperscript{40} Drones \textit{en masse} are the use of multiple drones without autonomous communication between the drones.

Drone-swarm technology is possible to increase/improve delivery of CR agents.\textsuperscript{41} The incident with a drone carrying a vial with a radioactive liquid that landed on the roof of the building where the office of the Japanese Prime Minister is, represents an example of future drones’ possibilities.\textsuperscript{42}

A possible scenario could be based on drones positioned on rooftops programmed to remotely take off at a given time, providing enough time to terrorists to escape the area or the country. In such a scenario the combination of chemical weapons with conventional munitions might trigger panic and chaos since responding to an attack while in personal protective equipment with limited dexterity, vision, and communication is not very effective. In a parallel scenario, a conventional drone attack might mask a simultaneous biological dispersal to a totally unprotected population. It is of note that most cities are not equipped with air defense systems capable to intercept or destroy drones as it was recently witnessed repeatedly times in London’s Gatwick and Heathrow airports.\textsuperscript{43}

It is worth considering that one or more drones can attack the incident command post supervising a chemical or radiological incident site not to mention their ability to interfere in communications by using sophisticated jamming equipment. The “aerial terrorist” of the future might also coordinate a swarm with a variety of specialized drones that will maximize the deadly consequences of the attack.

#### Hacking

The threat of cyber-attacks targeting chemical or nuclear facilities is a growing possibility.\textsuperscript{44} Given that chemical plants are now largely controlled by the use of networked computers, it is possible in some countries that cyber-attacks similar to the Stuxnet targeting of Iranian nuclear could cause critical systems failure.\textsuperscript{45} By hacking into computer networks, an adversary could
reprogram an industrial control system so that it commands the equipment to operate at unsafe speeds or opens valves when these should remain closed.46

Critical systems, like those of public utilities, transportation companies, and firms that use hazardous chemicals, need to be made much more secure. One analysis found that only about one-fifth of companies that use computers to control industrial machinery in the US even monitor their equipment to detect potential attacks - and that in 40% of the attacks they did catch, the intruder had been accessing the system for more than a year.47

The Internet

When it comes to terrorism, the internet is considered the proverbial Pandora’s box. Numerous websites, social media pages, and chat rooms in the world wide web and many more in the dark web provide information and detailed instructions, offer manuals and books about practically everything – from constructing an IED to how to produce ricin from castor beans at home.48 Not all sources on the internet are reliable but some can lead amateurs to the construction of a real weapon with the help of ingredients available over-the-counter or from suppliers on the internet. Is it possible to control the internet? Unfortunately, it is too late now in open societies – terrorists know that and we know that. What can be done to minimize the spread of malignant knowledge? Existing technologies make identification of internet interactions a very difficult and sometimes impossible task, given encryption and other hiding techniques.

Prevention

To prevent access to CBRNE weapons, government and corporate and other security actors must focus on a number of areas including theft and smuggling; rogue state trade; trafficking; scientist recruitment; orphan sources; the use of toxic industrial chemicals as weapons; dual biotechnologies; dirty bombs; nuclear trafficking; and the nexus of organized crime and terrorist organizations.

Theft and Smuggling

The Soviet Union’s chemical weapons program was in such disarray in the aftermath of the Cold War that some toxic and radioactive substances got into the hands of criminals or those who tried to sell these to them. While nerve agents degrade over time, if the precursor ingredients for nerve agents were smuggled out in the 1990s and stored under proper conditions and mixed more recently, these agents could still be deadly.

Attacking a nuclear power plant is difficult but not impossible. Terrorists could find a way to sabotage a plant, causing radiation to escape into the environment. In 1992, for example, a hacker named Oleg Savchuk was arrested for trying to sabotage the Ignalina Nuclear Power Plant in Lithuania using a computer virus.50

In August 2019, the Nuclear Threat Initiative (NTI) released an annual Global Incidents and Trafficking Database,51 produced by the James Martin Center for Nonproliferation Studies (CNS). In 2019 alone, CNS recorded 167 incidents in 23 countries where nuclear and other radioactive materials were found outside of a regulatory control regime (this was an increase from 156 incidents in 2018). Among them: the loss of 1g of weapons-gram plutonium from a university laboratory in the US. Trends remain consistent with the data collected between 2013 and 2017. In 2018, 58 losses were recorded while there were 45 thefts. 64 incidents occurred during transport.52
Rogue State Trade

According to a 2017 UN report, two North Korean shipments to a Syrian government agency responsible for the country’s chemical weapons program had been intercepted in a six months period. The goods were part of a Korea Mining Development Trading Corporation (KOMID) contract with Syria’s Scientific Studies and Research Centre (SSRC).

Trafficking

While Slovakia is not a likely target for chemical weapons attacks, the substances needed for such an attack may have been smuggled through the country due to its geographic position and close proximity with areas where trafficking flourish. The Slovak Police Corps along with the Ukrainian police have been cooperating in detecting illegal CBRN materials at the Slovak-Ukrainian border for several years.

In 2009, U.S. counterterrorism officials authenticated a video by an al Qaeda recruiter threatening to smuggle a biological weapon into the US via tunnels under the border with Mexico. Smuggling a modern nuclear weapon across a border would be almost as easy as people smuggling and would present no trouble for professional people or drug smugglers. Approximately 350,000 people have been smuggled across the US-Mexico border in a typical recent year. The main issues are portability, which is really about size and weight (similar to that of a man) and weight and the probability of detection. Simulations of detection of mock-up nuclear bombs have been carried out in red teaming exercises. In a widely reported stunt in 2002, ABC News smuggled a mock-up of a nuclear bomb (7 kg of depleted uranium shielded by a steel pipe with a lead lining) in a suitcase by rail from Austria to Turkey crossing several border checkpoints without inspection.

In its Dabiq magazine issue No 9 (p.77), one ISIS writer noted:

“Let me throw a hypothetical operation onto the table. The Islamic State has billions of dollars in the bank, as they call on their wilayah in Pakistan to purchase a nuclear device through weapons dealers with links to corrupt officials in the region. The weapon is then transported overland until it makes it to Libya, where the mujahidin move it south to Nigeria. Drug shipments from Columbia bound to Europe pass through West Africa, so moving other types of contraband from East to West is just as possible. The nuke and accompanying mujahidin arrive on the shorelines of South America and are transported through the porous borders of Central America before arriving in Mexico and up to the border with the US. From there it’s just a quick hop through a smuggling tunnel and hey presto, they’re mingling with another 12 million “illegal” aliens in America with a nuclear bomb in the trunk of their car.”

Such statements highlight the potential risks in relation to the trafficking of weapons of mass destruction.

Recruitment of Scientists

Recruitments of scientists with a CBRN background can take several forms: it could take place following religious conversion; it could be an act of revenge against a previous employer; or it could be an embittered individual. Furthermore, it could follow after a direct threat against his/her life or against family members or relatives; the result of an impending job loss; the outcome of a business deal, or could also be a case of promising support to a scientist’s
ambitions to make a new invention. For example, in 2014 when the Islamic State seized Mosul, geologist Suleiman al-Afiari was recruited and given the task to organize a supply chain for mustard gas, outfitting a small cluster of labs and workshops. He accepted because “I was afraid that I would lose my job. Government jobs are hard to get and it was important to hang on to it.”

**Orphan Sources**

‘Orphan sources’ are radioactive sources, which are not under regulatory control, or have never been regulated, or were left without attendance, were lost, placed at an inappropriate location, transferred without proper permission from the government or were stolen. An “orphan source” falling into the hands of a regular citizen may lead to lethal consequences for those who touch these or get close to these radioactive objects. An example of such a situation was a radioactive contamination of 249 people with cesium-137 which occurred in 1987 in Brazil, costing the lives of four persons when the Institute of Radiotherapy in the town of Goiania moved to a new location, abandoning old radiation equipment.

It should be mandatory to ensure that a radioactive source may only be used by individuals or enterprises who have proved to the state that they are capable of ensuring safety and security of the source. Governments should enforce accountancy and monitor and control all radioactive sources. Another preventive method is counteracting the potential threat of IRS (Industrial Radiation Sources) converted into the “orphan” category. The sources that may be abandoned are categorized as vulnerable. Vulnerable sources are those radioactive sources, which are presently under control, but such control is insufficient for ensuring continuous safety and security.

**Toxic Industrial Chemicals as Weapons**

Toxic industrial chemicals can also be used as weapons. For example, an industrial catastrophe took place in India in 1984 when 3,800 people were killed while more than 11,000 others were injured when methyl isocyanate was released from the Union Carbide India Ltd (UCIL) pesticide plant in Bhopal. While this was an accident, a deliberate attack on a chemical plant by terrorists might have an even larger effect.

The largest concern after the events of 11 September 2001 was for a while that chemical plants might be among the next targets. A terrorist could crash an aircraft or an armed drone against a chemical plant, resulting in the release of chemicals and expose the surrounding area to a plume of toxic gases. A bomb could damage storage tanks or transport vehicles carrying chemicals, releasing deadly toxins. Terrorists could get into an industrial plant and release toxic chemicals from within, or a disgruntled company employee could intentionally release toxic chemicals into the atmosphere. Most chemical plants around the globe are located close to urban areas; therefore, depending on the location, if toxic chemicals were released from one of those plants, as many as one million citizens could be killed, injured, or evacuated (US estimate). Approximately 850,000 U.S. businesses use, produce, or store toxic industrial chemicals (TICs).

Military or civilian food or water supplies could also be threatened, directly or indirectly, by a terrorist attack with TICs. Contaminating animal feed is an indirect method of poisoning the food supply, spreading toxins to people who eat contaminated animal products. Depending on the chemical, the residual toxins ingested by animals could be enough to cause mass illness and possibly even death within a meat-eating human population.
Dual Biotechnologies and Terrorists

Although the potential impact of a biological weapons attack can be significant, the likelihood is currently not believed to be high. Back in 1984, the Rajneeshee cult performed the first biological attack in the recent history of the US by poisoning with *Salmonella typhimurium* the salad bars of 10 restaurants in an effort to influence local elections in a town in Oregon. In 1993, the Aum Shinrikyo cult was involved in bioterrorism exploitation with *Bacillus anthracis* to be used against the citizens of Tokyo first with a homemade sprayer from the roof of a cult building located in a residential neighborhood and later from a modified truck. Days after the 9/11 massacre in 2001, five US citizens were killed and 17 got sick following exposure to *Bacillus anthracis* spores send by the regular mail service.

Genetic engineering, toxicology, molecular biology, and related sciences could contribute to the development of new generations of biological weapons by increasing the virulence and antibiotic resistance of pathogens, enhancing non-transmissible agents for airborne transmission and creating organisms or biological agents capable to attack humans and entire ecosystems.

The Biological and Toxin Weapons Convention (BTWC) entails prohibition of the development, production, stockpiling and acquisition of biological and toxin weapons. This convention is also apprehensive regarding the development of dual-use technologies in the areas of genetic engineering, biotechnology, and microbiology, for growth of products and processes that are capable of being used for purposes inconsistent with its objectives and provisions.

Rapid advances in gene editing and so-called “DIY biological laboratories” which could be used by extremists, threaten to derail efforts to prevent biological weapons from being used against civilian targets.

One might wonder why one should spend money and scientific expertise to create novel bio-weapons for which currently no defenses are available, when at this moment a dynamite-loaded properly loaded truck (VBIED), with or without chemicals or a radioisotope, could do much harm and produce the effect intended by terrorists at a reasonable cost? One possible answer could be found in the sphere of scientific ambition when a scientist turns mad. A gifted but frustrated scientist could cause havoc and spread a pandemic much more deadly than some of the known biological weapons of the past. A scientifically trained bioterrorist could get hold of the DNA of a virus and program it to disrupt or suppress certain cellular functions in human populations. He or she could also create chemical-resistant insects and then use these against the agricultural production of a country. Therefore, the scientific community, together with governments worldwide should create a framework regarding the extent and the depth of scientific research in critical areas because a rogue scientist might become terrorists too. This has apparently happened in the case of the anthrax attacks of 2001 in the United States. There Bruce E. Ivins, a microbiologist from a national biodefense laboratory, was found to be the chief suspect in the distribution of weapon-grade anthrax spores by mail. This is why better state supervision is mandatory - whether it is inside state, hospital, university or pharmaceutical industry laboratories.

Dirty Bombs and Terrorists

A “dirty bomb” or radiological dispersal device (RDD) is an explosive improvised device that combines conventional explosives, such as dynamite or C4, with radioactive materials. Most RDDs would not release enough radiation to kill more than a few people or cause severe illness. The conventional explosives would kill or injure more people in close proximity to the site of the explosion than the radioactive materials themselves. However, a RDD attack would create fear and panic, contaminate people and property, and require a costly cleanup. For “dispersal”
no explosives are needed. It could involve adding radioactive materials to a ventilation system (inhalation threat; expensive cleanup cost), spraying radioactive materials over a populated area with a crop duster or a drone, or contamination of water supplies (although the high dilution is not likely to result in individually significant injuries). In addition, radiological materials can be used in a radiation emitting device (RED, uncovered lead container) hidden in mass gathering places like a subway car or in the outpatient clinics department of a hospital. In addition, placing an IED in an area where radioisotopes are stored (nuclear medicine departments of hospitals) or used (cesium irradiators in hospitals’ blood banks or radiotherapy units) may result in an outcome similar to the one of exposure to a dirty bomb. A capsule of Cobalt 60 ($^{60}$Co) used for cancer treatment typically contains about 7.4·10^{13} \text{Bq} (2000 curie), which corresponds to a mass of about 1.8 grams.\textsuperscript{74} The same applies for sabotage of spent fuel transport cask and the corresponding release of radioactive aerosol.\textsuperscript{75}

Until now no dirty bombs have successfully been detonated. However, the threat is not imaginary. A vivid example is the 2008 case of the millionaire James Cummings. In his home in in Belfast, Maine, USA, police found both radiological materials and technical literature on how to construct a dirty bomb.\textsuperscript{76} Such a case indicates that the threat is real. Another example of potentially planned use was the discovery of explosives together with a radiological source (cesium-137) buried, by Chechen rebels, in the Izmailovsky Park in Moscow in 1995.\textsuperscript{77} For a terrorist organization with even rudimentary IED capabilities, the design and building of the explosive elements of a dirty bomb would be relatively easy. Obtaining radioactive material in sufficient quantities to create a major radiological dispersal is, however, a much harder challenge and one which can be countered by appropriate monitoring of radioactive sources, their regulation and effective law-enforcement.

**Improvised Nuclear Devices**

An Improvised Nuclear Device (IND) is a primitive type of nuclear weapon. When an IND explodes, it gives off four types of energy: a blast wave, intense light, heat, and radiation. The idea of terrorists accomplishing such a big bang is, unfortunately, not out of the question; it is far easier to make a crude, unsafe, unreliable nuclear explosive that might fit in the back of a truck than it is to make a safe, reliable weapon of known yield that can be delivered by missile or combat aircraft.\textsuperscript{78}

Could resourceful terrorists design and build a crude nuclear bomb if they had the needed nuclear material? Unfortunately, repeated examinations of this question by nuclear weapons experts in the US and elsewhere have concluded that the answer is yes – for either uranium or plutonium nuclear bomb, provided they can get hold of the required radioactive materials through theft or from trafficking.\textsuperscript{79}

**Nuclear Trafficking**

The Black Sea region is a vital strategic crossroads between Europe, Asia, Transcaucasia, Russia, and the Middle East, and has long been used for smuggling of licit and illicit goods, including nuclear materials since the end of the Cold War. Over 630 nuclear trafficking incidents were recorded in Black Sea states between 1991 and 2012, almost half of them in or from Russia. Five of the recorded incidents involved highly enriched uranium (HEU), raising concerns about the region’s use as a transit route for nuclear material smuggled from the former Soviet Union to the Middle East.\textsuperscript{80}

The seizures of HEU samples in Georgia in 2010,\textsuperscript{81} and Moldova in 2011,\textsuperscript{82} suggest that some quantities of previously stolen weapon-grade nuclear materials may still be available for
illegal transfer and sale to state and non-state actors. Therefore, it is important that efforts to
counter nuclear trafficking in the Black Sea region are continued and enhanced.

The terrorism-organized crime nexus could provide not only the basic nuclear material
required for a radiological dispersal device or an improvised nuclear bomb but even an actual
nuclear warhead to be delivered to the targeting site in the back of a truck or as payload of a
drone.

**IED – WMD Networks Nexus**

Convergence between IED facilitation and WMD proliferation networks could also potentially
lower existing thresholds, making the proliferation of WMD not only easier but more
widespread. Networks are composed of people, material, infrastructure, money/finance,
information, and lines of communications, which can be both physical and virtual. Perhaps the
most notable WMD proliferation network was Abdul Qadeer Khan’s nuclear technology
network which stood at the basis of Pakistan becoming a nuclear power currently possessing
more than 100 atomic bombs. While A.Q. Khan’s network sold critical technology he stole
from his time with URENCO in the Netherlands to state actors (e.g., Libya, North Korea)
from his base in Pakistan, the father of Pakistan’s atomic bomb could have sold know-how and
nuclear materials to non-state actors as well.83 This does not imply that a terrorist could easily
develop and employ a nuclear weapon, but rather that there are profit-minded suppliers willing
to sell crucial components to them.

In 2018, to respond to this new security environment and further restrict access to
dangerous substances, the European Commission proposed to strengthen the existing rules –
both online and offline sales.84 The proposed measures included:

1. Addition of new substances and concentration limits to the list of banned chemicals;
2. Inclusion on the list of economic operators of entities operating and selling online;
3. Background and criminal-record checks of public buyers;
4. Obligation to report a suspicious transaction within 24 hours; and
5. Greater awareness-raising and information sharing along the supply chain.

**Conclusion**

Attacks with CBRN materials and agents are not necessarily producing mass casualties or mass
destruction. However, even a small-scale attack can become a game-changer and spread the
fear pursued by all terrorists. It is a fact that a number of Islamist terrorist groups have
expressed an intention to use CBRN materials and use these offensively rather than just as a
deterrent. However, their capabilities are at the present time, in most cases, very low or non-
existent.

Looking at various probable scenarios, a chemical attack is most likely, followed by a
radiological attack. A serious biological offensive is currently beyond the means of most, and
probably all, existing terrorist groups without state support; the same is even more true for
detonating an improvised or stolen nuclear device. However, a suicidal attack on a nuclear
power plant or a radiological waste storage site is a distinct possibility, while an attack on a
chemical-industrial complex is even more probable.

In order to continue to be taken seriously, leading terrorist organizations like al Qaeda
might aim to produce an incident bigger than 9/11, and if they cannot do so in terms of
producing more casualties, they might seek a qualitative quantum jump with the help of CBRN
materials and agents, especially a radioactive dispersal device (a “dirty bomb”) which is likely
to cause a short-term psychological shock and long-lasting local contamination.
At the present time, there is only a very low risk of catastrophic biological and nuclear terrorism but it is nevertheless real. On the other hand, chemical and radioactive attacks are much more probable, but pose a lower risk of mass casualties. Nevertheless, response agencies need to address all threats and identify as many as possible gaps that might attract terrorists’ attention leading to an actual asymmetric attack. Appendix 1 list some preventive actions that ought to be taken to be prepared for both high risk and low probability events and high probability but low risk ones. This is followed by an Appendix listing some of the dual use problems on the horizon or already present when it comes to biological terrorism.

Ioannis Galatas is a retired Brigadier General in the Greek Army and as a military physician he specialized in Allergy and Clinical Immunology. Since 2001 he has been involved in CBRNE operations as planner and instructor and trained (including live agent training) in a number of countries abroad. During the 2004 Athens Olympic Games, he served as Commandant of the Olympic Hospital’s CBRN Response Unit. He holds an MSc. on “International Terrorism, Organized Crime and Global Security” (Coventry University, UK) and he is a Ph.D. candidate (Athens Medical School/ Forensics). His last assignment was as Head of the Dept. of Asymmetric Threats, J Mil Intel Service, HNDGS. Currently, he is the Editor-in-Chief of the online “C2BRNE Diary”; a Senior Research Associate at the Center for Security Studies, HMoI (Greece); a member of the Didactical Board of the University of Rome “Tor Vergata” for “International CBRNe Master” programs; a CBRN consultant, Emergency Department, Gemelli Policlinico, Catholic University of Sacred Heart, Rome (Italy); the Manager of the CBRN Knowledge Center, International CBNE Institute (Belgium), and a Senior CBRN Consultant at HotZone Solutions (The Netherlands).
Appendix

What can be done to Counter the Threat of CBRN Terrorism?

1. Intelligence collection priorities ought to focus strongly on proliferation issues associated with certain types of non-state actors such as jihadist movements, religious sects, racist groups and others who might be tempted to acquire weapons of mass destruction;
2. Trade in (precursor) materials for biological, chemical and nuclear substances must be subjected to better monitoring and greater control;
3. Existing conventions in the field of biological, chemical and nuclear weapons, terrorism and organized crime must be strengthened by adding (better) monitoring, implementation and sanction mechanisms;
4. International cooperation to counter proliferation and terrorism must be enhanced and bureaucratic “red tape and turf fighting” have to be minimized by creating more flexible and collaborative organizations;
5. Existing government stockpiles of nuclear weapons must be better guarded and accounted for, and ought to be gradually phased out or brought under international control. A credible multilateral nuclear disarmament program by governments will also put moral pressure on non-state actors to refrain from the acquisition of atomic weapons.

The major advantages of terrorists are the element of surprise and an innovative modus operandi since they are rapidly adjusting to countermeasures taken after each foiled attack. Surprise and innovation are two characteristics that cannot be easily matched. What can be done is the identification of gaps and vulnerabilities the same way terrorists are using these when planning their operations. Once we can leave behind us the deeply ingrained attitude that “it will not happen to us”, both the effects of surprise and innovation can be limited to acceptable and manageable levels.
Endnotes


2 Huggler, Justin, ‘Islamist extremist ricin plot foiled by German police,’ The Telegraph, 14 June 2018. Available at: https://www.telegraph.co.uk/news/2018/06/14/islamist-extremist-ricin-plot-foiled-german-police/; Andrew, Christopher, ‘Islamists have fled the battlefield… to plot mass murder with a dirty bomb,’ The Times, 24 June 2018. Available at: https://www.thetimes.co.uk/article/islamists-have-fled-the-battlefield-to-plot-mass-murder-with-a-dirty-bomb-8qtfsww82.


16 Biological attack scenarios: World Health Organization. Plague: 50-kilogram release over a city of five million could cause about 150,000 cases, or 36,000 deaths, in the first wave. A
secondary spread could cause a further 500,000 cases or 100,000 deaths. Tularemia: 50 kg over a city of 5 million could incapacitate 250,000 people and cause 19,000 deaths. Tularemia is highly infectious but not contagious. Source: Biological Threats and Terrorism: Assessing the Science and Response Capabilities: Workshop Summary. Institute of Medicine (US) Forum on Emerging Infections; Knobler SL, Mahmoud AAF, Pray LA, (eds.). Washington (DC): National Academies Press (US); 2002. Available at: https://www.ncbi.nlm.nih.gov/books/NBK98398/.


18 An IAEA expert noted that “The transfer of some Al Jesira process samples to Mosul University could explain the higher-than-expected uranium chemical inventory. Thus, the 40 kilograms of uranium chemicals “stolen” from Mosul University probable consist of lab reagents such as uranyl acetate (plus other species), yellowcake, ammonium diuranate, uranium trioxide, uranium dioxide and there might be samples of UCl4 uranium tetrachloride, but only gram quantities...” - The Mosul Mystery: The missing uranium and where it came from. The Guardian (2014). Available at: https://www.theguardian.com/world/julian-borger-global-security-blog/2014/jul/13/iraq-nuclear-mosul-uranium-isis.


21 Abu Musab al-Suri is a prominent Al-Qaeda member and author of the 1,600-pages long book The Global Islamic Resistance Call (Da’wat al-muqawamah al-islamiyyah al-’alamiyyah). He is considered by many as one of the most articulate exponents of jihad. He was captured by Pakistani security forces in 2005 was rendered to Syria. Cf. Brynjar Lia. Architect of Global Jihad. The Life of Al-Qaida Strategist Abu Mus’ab al-Suri. London: Hurst, 2007.


31 Treaty on the Non-Proliferation of Nuclear Weapons. UNODA. Available at: https://www.un.org/disarmament/wmd/nuclear/npt/.


33 Chemical Weapons Convention. Available at: https://www.opcw.org/chemical-weapons-convention

34 Hague Code of Conduct Against Ballistic Missile Proliferation. Available at: https://www.hcoc.at/.


36 Australia Group. Available at: https://australiagroup.net/en/.

37 Wassenaar Arrangement. Available at: https://www.wassenaar.org/.

38 Missile Technology Control Regime. Available at: https://mtcr.info/deutschziele/.

39 IoT Agenda. Drones. Available at: https://internetofthingsagenda.techtarget.com/definition/drone


41 Ibid.


48 Jihadist Manuals relating to CBRN and other weapons cover the following topics: The nuclear bomb of jihad and how to enrich uranium; nuclear weapons and their manufacture; ricin seeds; preparation of botulinum toxin; radioactive pollution; comprehensive course in poisons and poisonous gases; biological weapons; and the military jihad encyclopedia. Anne Stenersen and Brynjar Lia. Al-Qaida’s online CBRN manuals: A real threat? Oslo, Forsvarets forskningsinstitutt, 2007 (FFI-report 2007/02405), pp. 87-88 & p. 117. Available at: https://www.ffi.no/no/Publikasjoner/Documents/FFI-Fokus-2008-1.pdf.
50 “Computer Sabotage at Nuclear Power Plant.” Available at: https://www.risidata.com/Database/Detail/computer_sabotage_at_nuclear_power_plant.
52 Ibid. (from the James Martin Center’s 2018 report).
53 KOMID was blacklisted by the Council in 2009 and described as North Korea’s key arms dealer and exporter of equipment related to ballistic missiles and conventional weapons.
59 *Dabiq* was an online magazine produced by the Islamic State of Iraq and the Levant (ISIL) for Islamic radicalization and recruitment. It was first published in July 2014 in a number of different languages (including English). Its last issue circulated in July 2016.

68 Rajneeshee Bioterror Attack. Homeland Security Digital Library. Available at: https://www.hsdl.org/c/tl/rajneeshee-bioterror-attack/. Ironically, it was only discovered much later in the course of a criminal investigation that this food poisoning was deliberate.


70 Amerithrax or Anthrax Investigation. FBI. Available at: https://www.fbi.gov/history/famous-cases/amerithrax-or-anthrax-investigation

71 Biological and Toxin Weapons Convention. Available at: https://www.un.org/disarmament/wmd/bio/


73 A Canadian scientist funded by the American biotech company Tonix has demonstrated the possibility to create pox viruses from scratch. In this case, it was horsepox, a once-extinct virus resurrected by stitching together fragments of synthetic DNA to create an intact viral genome. The synthesis of horsepox virus was a significant accomplishment due to the large size of the virus and its complicated structure.


77 Lexi Krock and Rebecca Deusser. ‘Chronology of Dirty Bomb Events’. NOVA website. Available at: https://www.pbs.org/wgbh/nova/dirtybomb/chrono.html.


Bibliography


Andrew, Chr. (2018). ‘Islamists have fled the battlefield… to plot mass murder with a dirty bomb’. The Times (June 24, 2018). Available at: https://www.thetimes.co.uk/article/islamists-have-fled-the-battlefield-to-plot-mass-murder-with-a-dirty-bomb-8qtfsww82.


Test Program, Surrogate and Fission Product Aerosol Results’. (Nashville: Proceedings
of the 47th Meeting of the Institute of Nuclear Materials Management: Nashville, TN)
*Foreign Policy*. Available at: https://foreignpolicy.com/2010/01/25/al-qaedas-pursuit-of-
weapons-of-mass-destruction/
NATO website (2018). *Improvised Explosive Devices*. Available at:
https://www.nato.int/cps/en/natohq/topics_72809.htm
Pasha-Robinson, L. (2017). ‘North Korea caught sending shipments to Syrian chemical
weapons agency, reveals UN report’. *The Independent*. Available at:
https://www.independent.co.uk/news/world/asia/north-korea-syria-chemical-weapons-
sending-un-report-united-nations-nuclear-a7906951.html
Purver, R. (1995). ‘Chemical and Biological Terrorism: The Threat According to the
Open Literature’. *Canadian Security Intelligence Service."
Families*. RAN COE. Available at: https://ec.europa.eu/home-
affairs/sites/homeaffairs/files/ran_br_a4_m10_en.pdf
Smlama, S and Bursac, E. (2009). ‘Jihadist Capabilities and the Diffusion of
Knowledge’. In: Ackerman, G. and Tamsett, J. (eds.). *Jihadists and Weapons of Mass
Stenersen, A and Lia, B. (2007). ‘Al-Qaida’s online CBRN manuals: A real threat?’ Oslo:
FFI.
*Chemistry World*. Available at: www.rsc.org/chemistryworld/2015/06/chemicalplants-
vulnerable-cyber-attacks.
*CTC Sentinel*. Volume 10, Issue 9. Available at: https://ctc.usma.edu/the-evolution-of-
the-islamic-states-chemical-weapons-efforts/
Straub, J. (2019). ‘A cyberattack could wreak destruction comparable to a nuclear
Weapon.’ *Public Radio International* (PRI). Available at:
https://www.pri.org/stories/2019-08-16/cyberattack-could-wreak-destruction-
comparable-nuclear-weapon
Tabor, B. (2008). ‘Would it be possible for terrorists to smuggle a nuclear bomb across
the US-Mexican border if they ever got hold of one?’ *Quora.com*. Available at:
https://www.quora.com/Would-it-be-possible-for-terrorists-to-smuggle-a-nuclear-bomb-
Emerging Biological and Chemical Technologies’. Tucker, J.B. (ed.). The MIT Press,
2012, pp.19-44). Available at: https://muse.jhu.edu/book/20557
Turbiville, Graham H., “Weapons proliferation and organized crime: The Russian
Military and Security Force Dimension”, INSS Occasional Paper 10, Proliferation Series,
June 1996, US Air Force Academy, P. 37. Available at:
https://www.hsdl.org/?view&did=1148
guide for owners, operators, and chemical supply-chain professionals’ online. Available


Web-based Resources

CBRN Journals

- CBRNe World
- Chemical, Biological & Nuclear Warfare (CBNW)
- C²-BRNE Diary
- C-IED Report
- NCT Magazine

CBRN Organizations

- Australia Group
- CBRN Special Interest Group of World Association for Disaster and Emergency Medicine (WADEM)
- International Atomic Energy Agency (IAEA)
- Nuclear Suppliers Group
- Organization for the Prohibition of Chemical Weapons (OPCW)
- Stockholm International Peace Research Institute (SIPRI)
- United Nations:
  - United Nations Office for Disarmament Affairs (UNDA) – Biological Weapons
  - United Nations Office for Disarmament Affairs (UNDA) – Chemical Weapons
  - United Nations Office for Disarmament Affairs (UNDA) – Nuclear Weapons
  - UN Resolution 1540
- Wassenaar Arrangement

CBRN Centers of Excellence

- CBRN Network of Excellence
- Community of Users on Secure, Safe and Resilient Societies
- European Biosafety Association (EBSA)
- The European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative
- Global Initiative to Combat Nuclear Terrorism (GICNT)
- The International Forum to Advance First Responder Innovation
- The NATO Joint CBRN Defense Centre of Excellence

CBRN Training Centers

- Argon Electronics (UK)
- CBRN Defence Training Centre – Akademia Sztuki Wojennej (Poland)
- CBRN-E Training Centre, International Security and Emergency Management Institute, (Slovakia)
- Defence Chemical Biological Radiological and Nuclear Centre (DCBRNC) (UK)
• The European Nuclear Security Training Centre – EUSECTRA (Karlsruhe, DE and Ispra, IT)
• International CBRNE Institute (Belgium)
• Joint CBRN Defense Centre Of Excellence (Czech Republic)
• Seibersdorf Laboratories (IAEA, Austria)
• Serbian Armed Forces CBRN Centre (Serbia)

**CBRN Registered Training Organizations**

**Belgium**
- Centre de Technologies Moléculaires Appliquées (CTMA), Université Catholique de Louvain

**Czech Republic**
- National Institute for Nuclear, Chemical and Biological Protection

**Germany**
- The Bundeswehr Research Institute for Protective Technologies and CBRN Protection (WIS)
- Robert Koch Institute

**Italy**
- Observatory on Security and CBRNe Defense (OSDIFE)
- UNICRI – United Nations Interregional Crime and Justice Research Institute

**Netherlands**
- Netherlands Forensic Institute (NFI)
- TNO

**Norway**
- FFI

**Poland**
- Central Laboratory for Radiological Protection (CLOR)
- Faculty of Biology and Environmental Protection, University of Lodz
- Industrial Chemistry Research Institute (ICRI)
- Institute of Security Technologies MORATEX
- Military Institute of Hygiene and Epidemiology
- Military Institute of Chemistry and Radiology
- National Centre for Nuclear Research
- National Institute of Public Health – National Institute of Hygiene

**Sweden**
- European CBRNE Center, Umeå University
- FOI
UK
• Cranfield University

Ukraine
• International CBRN Risk Mitigation Research Center International

CBRNe Courses
• CBRNe Master Courses (Levels I and II) – Università di Roma “Tor Vergata”, IT
• The CBRN Defense Science Course – Cranfield University, UK
• CBRN Defense Courses – NATO SCHOOL Oberammergau, DE

E-Learning
• EU Non-Proliferation and Disarmament eLearning Course
• FLIR Primed
• Disaster Information Management Research Center – CBRNE (Chemical, Biological, Radiological, Nuclear and Explosives): Health Information Resources Training Modules
• A guide to effective chemical warfare agent training
• Project 10 of the EU CBRN CoE initiative – The online training course

CBRNE Portals
• CBRNE Central
• CBRNe Portal
• CBRNPro.net
• CHEMM – Chemical Hazards Emergency Medical Management
• Federation of American Scientists
• Global Biodefense – CBRNE Articles
• REMM – Radiation Emergency Medical Management
• The Homeland Defense and Security Information Analysis Center (HDIAC)

Free CBRN Software
• ALOHA
• Biodetection Guide for First Responders (iTunes)
• CAMEO fm
• CAMEO Chemicals
• Clinicians Biosecurity Resource (iTunes)
• Mobile REMM – Radiation Emergency Medical Management
• WISER – Wireless Information System for Emergency Responder
Chapter 18

Prevention of (Ab-) Use of Mass Media by Terrorists (and vice versa)

Alex P. Schmid

This chapter explores both the use of mass media by terrorists and the use of terrorism-generated news by mass media. Ever since the attention-raising effectiveness of “propaganda of the deed” was discovered in the second half of the 19th century, terrorists have exploited the mass media’s propensity to cover “bad news” extensively, first with the help of the rotary press, then followed by radio and television. Mass media, in turn, have often given broad coverage to terrorist attacks since the “human interest” generated by acts of demonstrative public violence attracts large audiences and generates extra revenue. There is a fine line between the media adhering to the public’s need to know, and broad media coverage creating exaggerated anxiety and thereby intimidating the public. Some existing media guidelines for covering terrorist news are discussed and evaluated with an eye on harm prevention resulting from the undue coverage of terrorist incidents.

Keywords: 9/11, Al Qaeda, audience, censorship, communication, contagion, guidelines, ISIS, jihad, mass media, media jihad, news, news values, propaganda of the deed, radicalization, television, terrorism
Modern terrorism is media terrorism. The media are attracted by extreme terrorist acts not only because it is their duty to report on any major event but also because the dramatic and spectacular aspect of terrorism fascinates the general public. Today’s terrorists exploit this and act in a way which will attract maximum attention around the world.


The terrorists need the media, and the media find in terrorism all the ingredients of an exciting story –

- Walter Laqueur (1999)

It has been said that terrorism is a combination of violence and communication. If one accepts this premise, the prevention of terrorism will have to focus on both violence and communication. The first question that arises is: how important is each of these two elements? Ayman al-Zawahiri, the current leader of Al-Qaeda wrote in 2005 in a letter to Abu Musab al-Zarqawi: “More than half of the battle is taking place on the battlefield of the media. We are in a media race for hearts and minds.” In the same vein, Osama Bin Laden wrote in a letter to Emir Al-Mominee: “It is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90% of the total preparation for the battles.” Shortly after 9/11, when Bin Laden was still publicly denying responsibility for the attack, he placed much of the blame on the Western mass media, but actually raised a valid point:

“The Western media is unleashing such a baseless propaganda, which makes us surprise[d] but it reflects on what is in their hearts and gradually they themselves become captive[s] of this propaganda. They become afraid of it and begin to cause harm to themselves. Terror is the most dreaded weapon in [the] modern age and the Western media is mercilessly using it against its own people. It can add fear and helplessness in the psyche of the people of Europe and the United States. It means that what the enemies of the United States cannot do, its media is doing that.”

The media in today’s world act very much like the nervous system of our societies. Yet, that alert system can be turned against the very social system it is meant to serve if it falls prey to misleading violent stimuli from terrorists (like those applied with the attacks of 9/11) and, through saturation coverage, magnifies single acts of terrorism to enormous proportions. Terrorist-made “bad news,” such as the attacks of 9/11, amplified by television and repeated again and again in the weeks, months and even years thereafter around the world, seems to act like an auto-immune disease that infects many viewers again and again, frightening some while stimulating others.

This chapter explores first how some militants have learned to use mass media for their purposes, how mass media, in turn, have made use of terrorist events, and how governments and some of the mass media are trying to prevent, or at least minimize, such exploitation through introducing guidelines and advocating selective censorship. While the main sources of concern today are the internet and social media, the traditional mass media – mainly printed press and television – still play a large role in the terrorist calculus to influence public opinion and humiliate and/or blackmail governments. While other chapters in this Handbook focus on social media, this one looks at the traditional mass media, i.e. press, radio, and television.
Propaganda of the Deed - How Terrorists seek to use Mass Media

While in France during the “Reign of Terror” (1793-1794), serial public executions of “enemies of the revolution” by the guillotine were used to create and spread terror, by the late 19th century, an emerging sensationalist press amplified the impact of individual terrorist bombings. Anarchist and social-revolutionary theorists and practitioners discovered that one could use demonstrative acts of public violence as a way to enter the news system. They called it “propaganda of [or: by] the deed.”

The convergence of violence and the media began in the second half of the 19th century when two inventions began to interact – dynamite (discovered in the 1862) and the rotary press (perfected in 1881). Anarchists, social-revolutionaries, as well as ethno-nationalists, soon discovered the potential of this confluence. Here is what an anarchist wrote in 1881 in the San Francisco paper “Truth”: “Truth is two cents a copy, dynamite is forty cents a pound. Buy them both, read one, use the other.” A German anarchist named Johannes Most who had emigrated to the US and also worked as a journalist wrote in 1885, “What is important is not solely these actions themselves but also the propagandistic effect they are able to achieve. Hence, we preach not only action in and for itself, but also action as propaganda.” This combination had been given the name “propaganda of the deed” (la propagande par le fait) by its inventors and practitioners. They explained the underlying logic in these terms:

- Mikhail Bakunin (1870): “we must spread our principles, not with words but with deeds, for this is the most popular, the most potent, and the most irresistible form of propaganda”;
- Errico Malatesta (1876): “the insurrectional deed destined to affirm socialist principles by acts, is the most efficacious means of propaganda”;
- Peter Kropotkin (1870s): “By actions which compel popular attention, the new idea seeps into people’s minds and wins converts. One such act may, in a few days, make more propaganda than a thousand pamphlets. Above all, it awakens the spirit of revolt…”
- Johannes Most (1884): “Everyone knows…that the more highly placed the one shot or blown up, and the more perfectly executed the attempt, the greater the propagandistic effect.

The “exemplary deed”, as “propaganda of the deed” was also called, was meant to act as a spark to awaken the spirit of revolt, show the masses that resistance to state repression was possible and make those in power fear that they might be next. By killing heads of state and government, ranging from the Russian Czar Alexander II in 1881 to the Italian King Umberto I in 1900, terrorists made headlines without paying a penny in advertising costs. With their assassinations, they found a way of accessing the world’s news system by deliberately creating “bad news.” The historian Daniel Boorstin observed in one of his works that the transition from news gathering to news making took place in the years between the World Wars. However, it can be argued that terrorists already discovered “news making” in the late 1870s. Boorstin coined the term “pseudo-events” to describe “the new kind of synthetic novelty which has flooded our experience.” In his view, a pseudo-event possesses the following characteristics:

1. “It is not spontaneous, but comes about because someone has planned or incited it;
2. It is planned primarily (not always exclusively) for the immediate purpose of being reported or reproduced. Therefore, its occurrence is arranged for the convenience of the reporting or reproducing media. Its success is measured by how widely it is reported.”

The Greek word *pseudo* means “false, meant to deceive.” Terrorists create “pseudo-events” which are real in their consequences for the direct victims, but which mainly serve to deceive
many others, manipulating them, for instance, into believing that the terrorists are much stronger than they really are. The earliest definition of terrorism, coming from ancient China, is “Kill one, frighten ten thousand.” With the advent of mass media, the force multiplication of terrorism became much larger and a single demonstrative public murder can scare or impress millions of people.

In a study with the title *Violence as Communication* (1982), I had argued that violence and propaganda have much in common. Propaganda aims at behaviour modification by coercion. Propaganda aims at the same by persuasion. Terrorism can be seen as a combination of the two. Eugen Hadamovsky, a Nazi radio director serving under Germany’s propaganda minister Joseph Goebbels, already noted in 1933 in his book *Propaganda and National Power* that “Propaganda and violence are never contradictions. Use of violence can be part of propaganda.” Terrorism, by using violence against one victim, seeks to coerce or persuade others. The immediate victim is merely instrumental - to use a crude but telling metaphor - the skin on a drum beaten to achieve a calculated impact on a wider audience. Violence always calls for attention as it is potentially life-threatening and we cannot ignore it, even if it is not taking place in our street but “only” in a radio broadcast or on the television screen.

Not only the National Socialists in the 1930s, but also Communist theorists like Carlos Marighella in the 1960s, recognized the utility of using a mix of violence and propaganda. In his *Minimanual of the Urban Guerrilla* (1969) the Brazilian terrorist theorist detailed how “propaganda of the deed” works:

1. Terrorist acts should be aimed at the audience, the general public;
2. Victims should be chosen for their symbolic meaning;
3. The media are eager to cover terrorist violence;
4. The media can be activated, directed, and manipulated for propagandistic effect;
5. Governments are at a disadvantage because their only choice is between censorship and letting terrorists make use of their media.

As a public display of power over life and death, many acts of terrorism are highly dramatic, almost irresistible for the media not to report. A German terrorist, Hans-Joachim Klein said: “If they do not listen to us, then we throw a couple of bombs.” On another occasion, he said: “We give the media what they need: newsworthy events. They cover us, explain our causes and this, unknowingly, legitimates us….” Ted Kaczynski, the Harvard-educated Unabomber, put it this way: “In order to get our message before the public with some chance of making a lasting impression, we’ve had to kill people.”

In other words, terrorists know what the news media consider “news value” and tailor (some of) their attacks to fit the criteria of the news system in order to get free publicity on a scale that very few could afford if the same prominent space and time in the media had to be bought in the form of advertisements. The media’s news value system puts a premium on things that are new, surprising, unexpected, dramatic, disruptive and have what is termed “human interest.” Many acts of terrorism fulfil half or more of the elements that commonly determine “news value” and therefore lead to publication:

1. Immediacy and event-orientation;
2. Drama and conflict;
3. Negativity (bad news has drama and conflict);
4. Human interest;
5. Photographability;
6. Simple story lines;
7. Topicality (current news frames);
8. Exclusivity;
9. Status and reliability of information source;
10. Local interest.23

By tailoring their violence to the news values of the media (e.g. “if it bleeds, it leads”),24 terrorists could - and still can - gain access to mass audiences. The media not only transmit their message – a deed that speaks for itself and/or a communiqué to go with it – almost in real time. They also publicize the terrorists’ grievances and accusations free of charge, which makes their strategy very cost-effective. Empirical research has shown that a number of goals are pursued in this way.

1. Winning or enlarging sympathy among “their” public;
2. Winning new recruits for the terrorist organization;
3. Demoralizing targeted sectors of the public;
4. Demonstrating the vulnerability of authorities;
5. Polarizing the political situation.25

The media have become a weapon of mass communication in political conflicts and even more so in armed conflicts. This is nothing new. The Nazi propaganda minister, Josef Goebbels, had already known that “News is a weapon of war. Its purpose is to wage war and not to give out information.”26

Each side in a conflict wishes to give a certain media “spin” to what is happening, so that pertinent events are interpreted favourably by one side or the other. Terrorists are primarily interested in the psychological rather than the physical effects of their violence, based on “…. their conviction that the actual effect of terror is its representation in the media, without which its value and effect as a weapon is meaningless and limited” - to quote the former Director of Israeli Television, David Witzhum.27 Satellite-linked live television has increased audiences to hundreds of millions and – today – even more. An attack on Israeli athletes at the Munich Olympic Games of 1972 reached an audience of up to 800 million television spectators.28 The Palestinian Liberation Organization leader Abu Iyad, Yassir Arafat’s deputy, explained one of the rationales behind this attack: “To exploit the unusual concentration of media coverage in Munich to give our struggle an international resonance – positive or negative, it didn’t matter....”29 Brian Jenkins, an American researcher, wrote in the mid-1970s: “Terrorism is aimed at the people watching, not the actual victims. Terrorism is theatre.”30

Once reported, such violent communications tend to terrorize segments of society which belong to the same category of people as the direct victims. The perpetrators of violence can at the same time also impress actual and potential constituencies of the terrorists and they can pressure governments to respond to the political demands of the terrorists. In other words, one act of violence, and even more so a series of acts of violence against non-combatant civilians, can alternatively impress, intimidate, or coerce different (but sometimes partly overlapping) target audiences.31

The 9/11 attacks served several purposes. In the words of Bin Laden (who had already announced in 1997 when asked about his future plans: “You’ll see them and hear about them in the media, God willing”32): “The effect of his deed [of one of the 9/11 hijacker-pilots] was significantly more efficient than many million books, which have been ‘written for the strengthening of Islam…. They [Al-Qaeda’s 9/11 hijackers] have not only destroyed the towers of the World Trade Center and the Pentagon. That would have been too easy. No, they have destroyed the symbol of the tyrants of our times and their values.”33

The main targets of these attacks were, however, not the near 3,000 people from more than 60 countries who died in the 9/11 attacks, or even the American people as a whole. In the words of one of the top commanders of Al-Qaeda, Saif al-Adel:
“...al Qaeda has, and always had, a specific aim: to arouse the sleeping body of the Islamic Nation – a billion Muslims worldwide – to fight against Western power and the contaminations of Western culture. In support of this aim, the 9/11 attacks were designed to force the Western snake to bite the sleeping body, and wake it up.”

The media were crucial in the calculus of Al-Qaeda and other jihadist groups. Faisal Devji, who analysed the speeches of Bin Laden and Al-Zawahiri in his book *Landscapes of the Jihad*, argues:

“Perhaps the most important way in which the jihad assumes its universality, however, is through the mass media. As a series of global effects the jihad is more a product of the media than it is of any local tradition or situation and school or lineage of Muslim authority. ... the jihad itself can be seen as an offspring of the media, composed as it is almost completely of pre-existing media themes, images and stereotypes. ... It is no exaggeration to say that only in this globally mediated landscape does Islam become universal, uniting Muslims and non-Muslims alike in a common visual practice.... The jihad battlefields become sites of a global Islam only when they are in the news, which is why combatants, funds, and supplies, not to mention the world’s attention, move from one battlefield to another, because the content of the jihad is the news itself as something new. ...Only in the mass media does the collective witnessing that defines martyrdom achieve its full effect, as the various attempts by would-be martyrs to film their deaths or at least to leave behind videotaped testaments, illustrates so clearly.”

The basic idea of “propaganda of the deed,” namely to openly perform acts of extraordinary violence to attract media attention and instrumentalize the publicity generated in an effort to gain leverage, has not changed much since the late 19th century.

Key is the triangular relationship between perpetrator(s), victim(s) and ultimate target(s) (see diagram ‘The Triangle of Terrorism’ in chapter 2).

With the help of mass media, terrorists can reach more than one “ultimate target.” One can distinguish at least ten different audiences:

1. Adversary (-ies) – usually government(s);
2. Society of the adversary;
3. Direct victims and their families and friends;
4. Others who have reason to fear that they might become next targets;
5. Members of the terrorist organization;
6. Members of other rival terrorist or political party organizations;
7. Constituency terrorists who claim to represent/act for the terrorist organization;
8. Potentially sympathetic sectors of domestic and foreign (diaspora) publics;
9. “Neutral,” distant publics;
10. Last, but not least: the mass and social media themselves.

Depending on what the intended purposes of a given act of terrorism are, an attack can be directed at one or several specific audiences. To create the connection between the direct victim and the ultimate target(s), however, the terrorist perpetrator needs mass media as amplifiers. Without them, the act of terrorism would not get much attention and the deed would be almost as unrecorded as the proverbial tree falling in the forest with nobody watching. A German terrorist, Bommi Baumann, member of the German left-wing urban guerrilla group 2 June Movement admitted, “Without journalistic reporting we would find ourselves facing a certain vacuum. It is through the press that our cause is maintained in the just manner ...”
Satellite-linked television, in particular, has given terrorism a new platform. In the words of Brigitte Nacos: “No other medium has provided more oxygen to terrorism than television because of its ability to report the news instantly, nonstop, and in visuals and words from any place to all parts of the globe, a facility that has affected the reporting patterns of other media as well.”

**How the Media Portray and (Ab-)Use Terrorism**

Since modern mass media came into existence in the second half of the 19th century, they have served several functions:

1. The *informational function* (updating the public about current events which might affect people);
2. The *interactional function* (providing an open forum for the free exchange of ideas and opinions); and
3. The *educational function* (transmitting useful knowledge to help define and clarify public issues).

However, pressured by the commercial character of many mass media and/or by their role in mobilizing public support for political parties in and out of government, two other functions have become stronger, often pushing the first three positive functions into the background:

4. The *political party function* (providing the public with preferred political judgments and ideological interpretations); and
5. The *commercial function* (obtaining more advertisements and increased sales and market shares for profit reasons to the media owners themselves).

Capturing a broad public and gaining and holding its attention is what most mass media in open societies have increasingly been looking for, driven by competitive market forces (“if we do not cover a terrorist incident to the fullest, the competition will, and audiences will switch TV channels”). The way to hold the attention of audiences is to provide the public with news, preferably with moving pictures, that has great “human interest.” The strongest human interest is the interest to survive. Any news that signals danger to survival is eagerly absorbed. Therefore “bad news” is more newsworthy than other news which signals no danger. This is sometimes described as “the basic news value.”

A closer look at news values and the place of “bad news” has been provided by Richard Hoggart. He had, in the mid-1970s, this to say about the journalism trade when television became the main source of news:

> “Of course, what they call ‘the news’ is biased; or, if that seems too loaded a word, artificially shaped. It is the result each day of a process of selection so speedy and habitual as to seem almost instinctive. … ‘The news’ selects itself by four main filtering processes. First, by simple constraints germane to the medium or fortuitously of the moment: constraints of available time or available resources, or of geography and so on. Second, ‘the news’ is decided by a tradition of ‘news values’ which television has largely taken over from the more popular end of the press and holds on to with little apparent will to think through their relevance, or irrelevance, to television’s own situation…. Third, there are what are known as specifically ‘television values’ or ‘television material.’ This item is recognized as good visually, so it rates a place before that; or this subject will be approached thus because that’s the angle which
makes ‘good television.’ The fourth and most important filter – since it partly contains the others – is the cultural air we breathe, the whole ideological atmosphere of our society, which tells us that some things can be said and others had best not be said. … By the concurrent and almost instant application of these four types of filter, television gives us what its practitioners call ‘the objective news’ but what is in reality a heavily-selected interpretation of events, one which structures reality for us, which shapes and frames a world for us to inhabit and accept as real and legitimated, one which sets the agenda within which – except by a positive effort at remaking – we are led to discuss the terms of our lives.”

In one sense “bad news” (e.g. about a killer on the loose in the neighbourhood) is “good news” since there is great local “human interest” in it and many people will switch on radio or TV to update themselves about a potential danger. For most mass media, such “bad news” is, commercially speaking, “good news” as it allows them to attract larger audiences which, in turn, generates larger revenues from advertisements. Hence the old journalistic adage: “Bad news is good news, good news is bad news, and no news is bad news.” Terrorists have discovered and continue to exploit this propensity of the news system and deliberately create “bad news.” This common interest of mass media and terrorists in “bad news” has been viewed by some observers as a form of “symbiosis.”

The historian Walter Laqueur once said that “the media are the terrorists best friend.” A German journalist turned academic, Brigitte Nacos, looking at the alleged symbiosis from the other side, described this relationship in these words, “[T]he news media and terrorists are not involved in a love story; they are strange bedfellows in a marriage of convenience.” On another occasion, she reformulated her statement: “All told, the mainstream media and terrorists are not bedfellows, they are more like partners in a marriage of convenience.” More recently, Jessica White also noted that: “… there is a clear synergy between the media’s desire for a sensational story and terrorists’ desire for publicity.” Both mass media and non-state terrorists want to obtain the attention of large publics, the terrorists to sell shock and awe to target audiences, the commercial mass media to sell large fearful publics to advertisers and reap the profits. Morality and profitability are sometimes at odds with each other when “news” is no longer primarily considered as a social and public good but treated as a commercial commodity like any other and packaged and marketed primarily to make money.

In an analysis of 21st century “propaganda of the deed” (POTD) Neville Bolt concluded in 2008 that:

“News organisations are trapped in a competition to deliver audiences; at the same time, they are caught in shrinking time and space. Reporting stories in real-time through twenty-four hour television news stations places them on an ever-shrinking timeline between event and broadcast. This timeline is governed by a number of factors. 1) The commoditisation of news and factual programming into a form of quasi entertainment creates viewer appetite. 2) The ‘tabloidisation’ of information means the most dramatic content rises to the top of the news running order, while the medium continues its ‘race to the bottom’. 3) The ubiquity and standardisation of formatted programming across television around the world means the underlying, tabloid visual grammar is shorthanded and homogenised, thus readily understood by any viewer. 4) The proliferation of state and commercial TV stations increases competition for the dramatic image and increases market-access for groups engaged in POTD. 5) The availability of low-cost technology means POTD group activity can be
relayed through ‘in house’ units of insurgents who record and edit attacks before making them available either on internet insurgency sites or via the web to global TV stations”.

In my earlier work, I had identified no fewer than thirty active and passive uses of the mass media by terrorists (see Appendix I). Three consequences of mass media reporting of acts of terrorism that stand out are briefly highlighted here.

**Intimidation**

Violence always demands our attention since it can be life-threatening. However, our instinctual reaction to pay attention to violence also works when the violence is not close to our immediate surroundings but “only” on television. Media-reported violence, especially when accompanied by graphic images, triggers our instinctive attention. Terrorists know that and so do mass media. The more media violence we are exposed to, the more people tend to become anxious, fearful or even terrorized, despite a certain numbing that can also be observed among parts of the public. Mass media, while informing us about violence, thereby can also intimidate us. That is perhaps the main effect of media portrayals of acts of terrorism. If mass media have a propensity to favour “bad news” over “good news”, the result is not just information but also intimidation.

**Agenda Setting**

By extensively covering certain news stories more than others, the mass media have the ability to determine the importance of issues in the public domain. What the public perceive as important becomes, in democratic societies, politically important, and sets the government’s agenda. A social issue becomes a political issue by receiving widespread media coverage. Such agenda-setting coverage, in turn, can be achieved by attacking people whose death is newsworthy. One tactical victory of non-state terrorists is that they can place issues on the political agenda and force governments to react – and often overreact. Acts of terrorism can set in motion a chain of events in a fertile surrounding, e.g., the nationalist revolt against empires in the early 20th century. The worst example is the assassination of the Austrian heir to the throne, Archduke Franz Ferdinand in Sarajevo on 28 June 1914 by the 19-year-old Bosnian Serb student Gavrilo Princip, who was linked to the nationalist Serbian Black Hand Organization. His assassination started a chain reaction of ill-considered governmental policy decisions in Germany, Austria, Russia, the UK, and France, leading to the outbreak of the First World War on 1 August 1914. When the war ended, the Austrian-Hungarian empire, the German empire, the Russian empire, and the Ottoman empire had crumbled. While this was an exceptional outcome, terrorists often can, with calculated assassinations and massacres, determine a government’s political agenda for months and years.

Acts of terrorism are often acts of provocation and in political party systems politicians often feel tempted to “play politics” with terrorism, calling for stronger counter-measures than the opposition. This process of outbidding between government and opposition following a terrorist attack can keep terrorism on the political agenda for weeks and months. Counter-measures targeting the constituency terrorists come from, tend to drive other members of the constituency into the arms of the terrorist organisation, making the constituency a “suspect community” in the eyes of other members of society, thereby leading to polarization and radicalization on both sides. A climate of suspicion and fear can be the result, leading to an escalation of violence. The way mass media reports on acts of terrorism often increase the risk of escalation.
Contagion

One probable effect of massive media reporting is contagion – a chain reaction of imitative acts by persons influenced by a reported successful initial act. While the majority of people reject violence and sympathize with the victims of terrorism, there are others who identify with the terrorists, approving their goals if not their methods. There is also a tiny minority who feel inspired and join a terrorist group or seek to copy acts of terrorism without direct links to the original perpetrators. Human beings have a tendency to imitate other human beings, and while such imitation is usually harmless – as in fashion trends that become popular – there are also harmful ones, as in copycat crimes and lone actor attacks. People learn from each other but also from the mass media; especially visual media like television can create captivating images that appeal to some to go out and do likewise. When mass media reach hundreds of millions of people, even the most atrocious acts of violence portrayed by mass media can find some eager learners and impressed imitators.

It is widely accepted by the mass media that detailed and graphic reports on suicides lead to more suicides of the same type. Most mass media have learned to be restrained in their coverage of suicides or do not cover them at all. However, this has not been true for suicide terrorism nor for other forms of terrorism like hijackings or ramming heavy vehicles into crowds of people. There have been various statistical studies that have shown a causal link between reporting on acts of terrorism and further similar acts of terrorism. One statistical study by Michael Jetter found that enhanced media attention to terrorism tends to lead to more terrorism. Other studies using different methodologies have noted similar contagion effects. This is exactly in line with what the inventors of “propaganda of the deed” in the late 19th century expected. Terrorists learn from each other and imitate each other but much of that learning is by means of mass media and, more recently, also from social media. In a chapter on Media-Induced Contagion of Terrorist Violence in the volume Violence as Communication, I described ten cases of serial contagion, and concluded that:

“The media can provide the potential terrorist with all the ingredients that are necessary to engage in this type of [imitative] violence. They can reduce inhibitions against the use of violence, they can offer models and know-how to potential terrorists and they can motivate them in various ways”.

In the 1970s, one of the tactics frequently used by terrorists was the occupation of foreign embassies. In one case – the occupation of the US embassy in Tehran on 4 November 1979, 52 hostages were held for 444 days, with some major mass media in North America covering the story on an almost daily basis. In an earlier study ten years after the events, I wrote:

“Terrorists use the media and the media use terrorism. At the time of the Tehran embassy incident this was particularly evident when the Canadian Broadcasting Corporation filmed a mob demonstration. As soon as the cameras were on, the demonstrators began shouting ‘Death to Carter’, raised their fists, looked angry and burned American flags. After two minutes, the cameraman signalled the end of the ‘take’. Then the same scene was done once more for the French-speaking Canadians, with the crown shouting ‘Mort a Carter’.”

Here the line between the television media’s news gathering and news making had clearly been crossed. The excessive media coverage of the hostage drama in the US embassy arguably cost President Jimmy Carter the re-election and brought Ronald Reagan into the White House.
In a globalizing world interlinked by satellite television, local terrorist acts can, and often do, assume global relevance. In study I did in 1992 I concluded:

“The rise of the newsworthy violent pseudo-event has, in my opinion, begun to poison journalism. It has started a feedback process in which the media, and television in particular, reflect reality less than reality has begun to reflect television’s news values. The implications of this shift from neutral news gathering to calculated news making by actors in and recorders of events are profound for the global electronic village.”

Some quality media have in recent decades developed guidelines on how to cover terrorist events, partly driven by apprehension that if the media would not police themselves, the government might do so with a heavier hand. It is to the issue of media guidelines we turn next.

**Media Guidelines to Prevent Terrorist (Ab-) Use of Mass Media**

The evidence that mass media reporting can facilitate terrorism is no longer seriously contested. Jessica White, a former intelligence analyst, for instance, concluded in a RUSI review of literature on media and terrorism in 2020 that:

“…. there is significant empirical evidence in the literature to suggest that the media can and sometimes does contribute to radicalisation, recruitment, mobilisation to violence and imitation of terrorist attack methods. …Media coverage of terrorism in any form amplifies the effects of terrorism, because it broadcasts attacks to a larger audience than would be immediately affected. … Analysis also indicates that inadvertent advancement does occur, due to the communication of terrorism through reporting.”

What then should – and can – be done to ban or at least minimize terrorist news making? One answer is governmental censorship (which we will not explore here), another answer is self-control by the mass media in the form of internal or inter-media guidelines advocating restraint in the coverage of terrorism. Relying on sound principles of news coverage antedates the current wave of terrorist exploitation of news values. Over the last century a set of journalistic ethical principles have emerged in Western democracies among quality papers and some visual media, which includes the following basic elements:

1. “to report truthfully, that is, honestly, accurately, objectively, and reliably;
2. to report comprehensively so that the public gets the best information available in order to develop an understanding of conflicting viewpoints and to reduce ignorance of significant issues;
3. to report impartially, that is, with fairness to all sides who have a point;
4. to maintain editorial independence against all interest groups;
5. to separate news from commentary so that a journalist’s bias towards a person or institution does not influence a news report.”

However, such principles – even when observed - are not a sufficient defence against abuse by terrorists, since these principles are largely based on journalistic news gathering rather than malicious news making by terrorists eager to capture public attention.

Individual media, media organizations as well as inter-governmental committees have tried to regulate media reporting in situations of terrorist campaigns since the 1970s. One of the first
was the British Broadcasting Corporation (BBC) when facing terrorist attacks in Northern Ireland and in Brighton, Birmingham, and London. Several news organizations and news agencies (e.g. Reuters) and individual editors have developed guidelines referring to issues such as:

- Coverage should be restricted to “facts” but must not imply encouragement, glorification, or condoning of acts of terrorism;
- News should not be presented in a way as to cause unnecessary panic, alarm, or stress;
- Increased attention should be given to humanizing the victims;
- Reduction in the prominence of imagery of the perpetrators;
- Promotion of narratives of community and cross-community solidarity.

Guidelines have also been proposed by independent observers. A good set comes from Raphael Cohen-Almagor from the University of Haifa, Israel. In 2005 he proposed, inter alia, the following ten guidelines:

1. The media should refrain from sensational and panicky headlines, from inflammatory catchwords, and from needless repletion of photos from bloody scenes. …
2. The media should not broadcast live terrorist incidents that include hostage taking. …
3. The media are advised not to interview terrorists while the terrorist incident is still in motion. …
4. The media are required to show sensitivity to the victims and to their loved ones. …
5. The media are advised to co-operate with the government when human lives are at stake in order to bring a peaceful end to the terrorist episode. …
6. Terrorism should be explicitly condemned for its brutality and violent, indiscriminate nature. …
7. The media should not jeopardize human life.
8. The media must not pay or be paid for covering terrorist incidents.
9. The media need to be accountable for the consequences of their coverage.
10. The media should not co-operate with terrorists who stage events.

These are valid points but one problem with such policy guidelines is that they are voluntary. When a major terrorist event becomes “breaking news,” and television networks compete with each other for scoops, the responsibility alluded to in such guidelines often tends to be forgotten. Furthermore, points 8, 9, and 10 of this list are linked to the very structure and functioning of many commercial as well as public mass media in open societies. As to point 8 (“The media must not pay or be paid for covering terrorist incidents”): If the coverage of terrorist incidents leads to a greater audience and as a consequence for commercial mass media, to greater revenues from advertisements, the payment to the media is invisible because it is indirect – coming not from the terrorists themselves but those who place advertisements next to terrorist news.

As to point 9 (“The media need to be accountable for the consequences of their coverage”): While careless terrorist news coverage has cost the lives of hostages, I can remember no instance where mass media or individual journalists have been held accountable for the loss of lives and had to pay indemnities to the families of victims or where editors or journalists went to prison as a consequence of irresponsible reporting. One reason for this is that it is often difficult to establish a direct chain of causation between careless media coverage and loss of human lives, at least in a form that would stand up in court.

The crux of the matter, however, is point 10 (“The media should not co-operate with terrorists who stage events”): Since acts of terrorism are almost by definition “staged” propaganda performances with the goal of catching the attention of the mass media, the very
act of reporting acts of terrorism amounts, de facto, to sometimes unwitting, and sometimes unwilling “co-operation.” In the words of Paul Wilkinson, “…. the free media in an open society are particularly vulnerable to exploitation and manipulation by ruthless terrorist organisations.”

Paradoxically, while terrorists use the mass media, they do not treat journalists with any regard. In fact, journalists have been kidnapped and killed by terrorists. One example is Daniel Pearl, an Israeli-American journalist for the Wall Street Journal. He was kidnapped in Karachi and beheaded in January 2002 by Khalid Sheik Mohammed, who was also the original planner of the 9/11 attacks. A British journalist, John H. Cantlie, was forced to become a “news” presenter for ISIS after being kidnapped in 2014, while the American journalist James Foley, who had been abducted with Cantlie in Syria, was beheaded by ISIS in August 2014, when a ransom demand of €100 million euros for his release was not met, with ISIS distributing a video about his killing.

In reaction to such events, a number of journalists and editors of mass media outlets have sought ways of denying individual terrorists publicity, for instance, by not mentioning their names or not showing their photographs or video clips, something called a “partial blackout” of news (as partly occurred in the case of the Christchurch attacker in New Zealand). However, given the competitiveness of the media business, such information often reaches the public, or parts of it, though on a smaller scale. Between self-censorship by the media and saturation coverage, there are many degrees of using or not using “bad news” created by terrorists. In this context, it should also not be forgotten that governments and politicians in and out of government also use terrorist events to push certain policy preferences (and sometimes their own careers). The media are not neutral but parties in the fight between terrorists, government, and society. They are the battleground in which terrorists and counter-terrorists fight to shape public opinion and special audiences’ perceptions with words and images about manufactured and real deeds and misdeeds.

Conclusion

How can such use and abuse of mass media by terrorists be prevented? This brings us back to the statement by the current leader of Al-Qaeda, quoted at the beginning of this chapter: “More than half of the battle is taking place on the battlefield of the media. We are in a media race for hearts and minds.”

The simple answer to the question of how abuse of mass media can be prevented is overt or covert mass media censorship by the government (for arguments for and against censoring terrorist news, see Appendix 2). Used with a heavy hand, censorship can close open societies. Katherine Graham, the former owner of the Washington Post, rightly noted in 1994:

“Publicity may be the oxygen of terrorists. But I say this: News is the lifeblood of liberty. If the terrorists succeed in depriving us of freedom, their victory will be far greater than they ever hoped and far worse than we ever feared. Let it never come to pass.”

Unfortunately, many governments have gone down the path of censorship, especially since 9/11. If the public debate in and through the media is repressed, democracy suffocates. The number of true democracies has gone down since 2006. According to The Economist’s Annual Democracy Index, there were in 2019 only 22 “full democracies” left, with only 5.7 percent of the world population enjoying full freedom, while more than one third of all human beings have to live under authoritarian regimes and the rest in only partly free countries.
Many governments have used the argument that censorship is necessary to prevent and control terrorism, but this argument has often been used to curb freedom of the press for other reasons as well. In many countries, especially in the Middle East and North Africa, free democratic public space has come under great pressure, with terrorists on the one side and repressive governments on the other. The control of the mass media through censorship or other measures, which also muzzles free expression in non-democratic regimes, has partly been circumvented by the terrorists through their shift to social media and other channels on the internet, which are harder to control than local television stations and print publishing houses. Yet, the traditional media remain important when it comes to terrorist propaganda as they often pick up information from the internet, turning it into “bad news.”

This brings us back to the question on how to deal with terrorist-made “bad news.” The rise of the newsworthy violent “pseudo-event” has poisoned journalism. It has started a feedback process in which the media, television in particular, are less reflective of reality than reality has begun to adapt to certain visual news values. The implications of this shift from neutral news gathering to calculated news-making by violent actors (as well as others) are profound for global society, for which the media function as its nervous system.

Mass media should not be prevented from reporting naturally occurring bad news, whether lethal or not. Yet in order to prevent, or at least reduce, abuse by terrorists, ways have to be found to minimize the intrusion of artificially created violent events that are crafted for appealing to the existing news value system and meant, on the one hand, to shock and intimidate the majority of the public and, on the other hand, among those who identify with the cause of the terrorists, attract and radicalize a small but not insignificant sector of violence-prone individuals in our societies.

Mass media are not neutral in the fight between terrorists and societies: they are, as we found earlier, the battleground, and as such, part of the problem. Yet they could also be part of the solution, a solution not based on censorship but on the understanding that if civilians get brazenly killed by terrorist groups to obtain publicity, to intimidate the public, or to coerce the government, the usual news values and practices (“bad news is good news” and “if it bleeds, it leads”) should no longer be automatically applied. A temporary blackout or at least minimizing such news could save lives, prevent copycat crimes, and help denying terrorists the attention and recognition they crave. Yet to achieve that, a reconsideration of what mass media consider to be “news” and what should constitute legitimate “news value” is necessary. When the public’s freedom of information becomes a freedom for terrorists to intimidate the public through pre-designed shocking acts of violence, something has clearly gone wrong and needs to be set right. Editors in the mass media should clearly distinguish between “genuine violence” that would have been inevitable, and “histrionic violence” for audience manipulation via mass media. Whenever the latter is suspected, coverage - at least visual coverage - should be minimal, if not entirely absent. While the public has, in democratic societies, a right to know, it should also realise that there are aggressive terrorists out there who seek to have our minds capitivated by messages of intimidation administered to us be mass media under the guise of freedom of information.

Responsible journalism should be responsible not to the terrorist desire for propaganda and the media corporations desire for profit first and foremost, but to public concerns, government concerns, and last but not least, victims’ concerns. The mass media do more than inform us when reporting on terrorism. They give tiny numbers of violent individuals access to millions of homes and allow the terrorist newsmakers to horrify us by sudden unprovoked killings of innocent people. In fact, we become secondary victims, some of us more than others, depending on the degree of identification with the primary victims.

Charlie Beckett from New York Columbia University’s Graduate School of Journalism has correctly noted that,
“The fact news media gives publicity to the terrorist is a problem that cannot be completely resolved. But journalism can be created in ways that reduce the propaganda effect for either the terrorist or the panicked politician. …The social impact of news coverage should be considered, not just audience numbers and the drama of the event”. 79

Research on mass media and violence in general and terrorism in particular has demonstrated that many people learn from the media and some imitate what they see in the media. The number of those who learn violence and imitate acts of violence seen in the media is small but not insignificant. Violence that is predictable is violence that is preventable. When it comes to terrorist violence, this places an obligation on those who work for mass media to carry their share of social responsibility in a whole-of-society effort to prevent terrorism by rethinking how to deal with terrorist-made “bad news.”

Alex P. Schmid is a Research Fellow at the International Centre for Counter-Terrorism (ICCT) in the Hague, the Netherlands. He is Editor-in-Chief of Perspectives on Terrorism and former Co-Editor of Terrorism and Political Violence – both leading journals in the field of Terrorism Studies. Until 2009, Prof. em. Schmid held a chair in International Relations at the University of St. Andrews where he was also Director of the Centre for the Study of Terrorism and Political Violence (CSTPV). Previous positions include Officer-in-Charge of the Terrorism Prevention Branch of the UN Office on Drugs and Crime in Vienna and a chair in Conflict Resolution at the Erasmus University Rotterdam. Between 1978 and 2018 he also held various positions at Leiden University. Currently, he is Director of the Vienna-based Terrorism Research Initiative (TRI), a consortium of 16 institutes and more than 100 individual scholars seeking to enhance human security through collaborative research. Alex Schmid has more than 200 publication and reports in ten languages to his name, including the award-winning volume “Political Terrorism” (1984, 1988, 2006) and the “Routledge Handbook of Terrorism Research” (2011, 2013).
Appendix 1: Active and Passive Uses of Media by Non-State Terrorists

1. Communication of (fear-)messages to mass audiences.
2. Polarizing public opinion.
3. Making converts, attracting new members to terrorist movements.
4. Demanding publication of manifestos under threat of harm to victims.
5. Using media as a conduit for threats, demands, and bargaining messages.
6. Verifying demand compliance by the enemy.
7. Winning favourable publicity via released hostages.
8. Linking message to victim.
10. Winning publicity by granting underground interviews.
11. Intimidating media by killing or wounding journalists.
12. Advertising terrorist movements and representing their cause.
13. Arousing public concern for victims to pressure governments to make concessions.
14. Discrediting victims by making their “confessions” public.
16. Deflecting public attention from disliked issues by bombing it from front pages.
17. Announcing further actions.
18. Using journalists as negotiators in bargaining situations.
19. Inciting the public against the government.
20. Occupying broadcasting stations to issue messages.
22. Gaining “Robin Hood” image.
23. Using media as an external communication network between terrorists.
24. Learning new coercive techniques from media reports on terrorism.
26. Obtaining information on countermeasures by security forces.
27. Using media at the site of siege as insurance against “dirty tricks” by security forces.
28. Creating fear among the enemies by media’s exaggeration of own strength, thereby reducing likelihood that individual policemen dare to apprehend terrorists.
29. Identifying future targets for terroristic violence.
30. Obtaining information about public reaction to terroristic acts.
Appendix 2: Arguments for and against Censorship

Arguments for Censorship

1. Non-state terrorists use the mass media as a platform for political propaganda, which also helps them to recruit new members to their movement.
2. Since publicity is a major, and in some cases, the sole reward sought by terrorists, censorship would make terrorism a less desirable strategy.
3. Detailed coverage of incidents by the media provides potential terrorists with a model that increases their chance of success in their own acts.
4. Reporting on acts of terrorism can produce imitative acts.
5. People who have so little respect for other people’s lives as terrorists do, should not be enabled to command public attention only because they use violence.
6. Media reports on terrorist outrages might lead to vigilantism and uncontrolled revenge acts against the group the terrorists claim to speak for.
7. Negative news demoralizes the public while “good news makes us good.”

Arguments against Censorship

1. If the media would keep quiet on terrorist atrocities, the violent terrorists might be judged less negatively by sections of the public.
2. Political terrorists boycotted by the media might step up their level of violence until the media have to cover their deeds.
3. If the media did not report on terrorism, rumours would spread, which might be worse than the worst media reporting.
4. Suppression of news on terrorism might leave the public with a false sense of security.
5. People would be unprepared to deal with terrorism, when directly faced with it.
6. If the media would censor terrorism, the public would suspect that other things are censored as well and the credibility of the media would decline.
7. The lack of public awareness of certain terroristic activities would keep the public from fully understanding the political situation.
8. The assertion of insurgent terrorists that democratic states are not really free would gain added credibility if the freedom of the press were suspended.81
Endnotes


7 The communication researcher Ben Bagdikian noted in the early 1970s when satellite-supported TV started to spread worldwide: “For most of the people of the world, for most of the events in the world, what the news system does not transmit did not happen. To that extent, the world and its inhabitants are what the news media say they are.” See Bagdikian, Ben H., The Information Machines: Their Impact on Men and the Media. New York: Harper & Row, 1971, pp. xii-xiii.


13 In his study of the origins of the “propaganda of the deed,” Fabian Lemmes noted, “…above all, a broad resonance space opened up for assassinations and those who committed these. The hitherto unparalleled transnational wave of assassinations in the ‘long’ 1890s cannot be explained without the massive, even abundant, reporting by the media of the late 19th century. By means of the enormous mediatisation, demonstrative violence as a political instrument relying on public attention generation gained its attraction. In addition, the constant presence of the topic in the public discourse across national boundaries inspired more perpetrators to engage in acts of imitation and revenge.” See Fabian Lemmes, ‘Propaganda der Tat. Zur Geschichte einer besonderen Gewaltpraxis,’ [Propaganda of the Deed. On the history of a particular violence practice] Mittelweg 36, Zeitschrift des


Schmid, Alex P. and Janny de Graaf, Insurgent Terrorism and the Western News Media. An Exploratory Analysis with a Dutch Case Study. Leiden, COMT, 1980, p. 44.


“Leads” refers here to be placed on page one of a newspaper. Already in the 1950s, FLN leader Ramdane Abane instructed his followers in the struggle for the liberation of Algeria from France: “We must have blood in the headlines of all the newspapers.” See: Crenshaw Hutchinson, Martha, Revolutionary Terrorism: The FLN in Algeria, 1954-1962. Stanford, Hoover Institution Press, 1978, p. 94.


Witzhum, David, op. cit., p. 33. – This is echoed in the statement, “Yet as a weapon, terror is sophisticated. It is “1% bang and 99% publicity.” See Simon Jenkins, ‘Reviewing Matthew
31 Terrorism does not “terrorise” everybody, but only the direct victims and those who strongly identify with them. There is a whole spectrum of different reactions to acts of terrorism from very negative to very positive, depending with whom a witness or indirect observer identifies: the victims, the terrorists, the government, or someone else. The individual scale of reactions to acts of terrorism includes those who are: 1) terrorised and intimidated; 2) panicking and confused; 3) frightened and showing loss of confidence; 4) worrying and distressed; 5) angered, with hardened opposition to the terrorist cause; 6) indifferent or wavering; 7) positively impressed by short-term impact of terrorist act; 8) sympathetic to terrorist cause; 9) supportive of terrorist tactics; 10) seeking to join terrorist organization. After 9/11, some of the reactions listed under points 7 to 10 were not unusual in the Arab world. Cf. Schmid, Alex P., ‘Public Opinion Survey Data to Measure Sympathy and Support for Islamist Terrorism: A Look at Muslim Opinions on Al Qaeda and IS,’ The International Centre for Counter-Terrorism (ICCT) Research Paper, February 2017. Available at: https://doi.org/10.19165/2017.1.02.
33 Quoted from a 62-minute video produced by Al-Qaeda’s propaganda committee, as quoted in Der Spiegel (Hamburg), 44, 27 October 2003, pp. 122-123.
36 In an analysis from 2008, Neville Bolt wrote about Propaganda of the Deed (POTD), “POTD is more than an operational technique intended to produce ‘shock and awe’ through the force multiplying effect of fear. (…) POTD is a symbolic and rhetorical tool for insurgents in a repertoire of ‘political marketing’ – it encourages the formation of sympathetic support-communities. (…) POTD has shifted from territorial to ‘virtual’ theatres of operation.” See Bolt, Betz, and Azari, 2008.
38 This list is not exhaustive. Some terrorists might, unconsciously perhaps, aim for a boomerang effect. As I wrote elsewhere, “In fact, I suspect that in many cases the terrorists and their immediate supporters are the only ones who appreciate the results of their violence. Auto-propaganda, whereby the terrorists are both perpetrators and chief audience, is a very important element. A bomb set off, an opponent killed, and the media coverage that goes with it boost their morale much more than it lowers that of their opponent. The terrorist message to the ‘true believers’ - the community of insiders – might be more important than the message to the outsiders.” See Schmid, Alex P. ‘Terrorism and the Media: Freedom of Information vs. Freedom from Intimidation’; in: Howard, Lawrence (ed.) Terrorism. Roots, Impact, Responses. New York: Praeger, 1992, p. 106.
40 Ted Koppel, an anchor man of the ABC TEV network in the United States has been quoted as saying, “Without television, terrorism becomes rather like the philosopher’s hypothetical tree falling in the forest: no one hears it fall and therefore it has no reason for being. And
television, without terrorism, while not deprived of all interesting things in the world, is nonetheless deprived of one of the most interesting.” Cit. Anzovin, Steven, _Terrorism_. New York, NY: H W Wilson, 1986, p. 97.


43 This list (which is not the author’s own creation but taken from communication studies) is not exhaustive. There is at least one more function: 6) recreational function (providing entertainment and amusement about the ways of society). There are also combinations of functions. In this context, Brigitte Nacos noted: “As serious news organizations move increasingly away from reporting what journalists/gatekeepers deem important for the enlightenment of fellow citizens to what profit-oriented corporate managers consider interesting for the entertainment of news consumers, “hard” news is increasingly crowded out by “soft” news. … As a result, most news offered in the twenty-first century is essentially a blend between “hard” information and “soft” entertainment – infotainment in the guise of news reporting. … Infotainment, far more than informative hard news, strives on the very images and themes that terrorist incidents offer – drama, tragedy, shock, anger, grief, fear, panic – the ideal ingredients for transforming real life terror into breath-taking thrillers or heart-breaking soap operas designed to captivate and stir up audiences.” – Nacos 2002, pp. 28-29.

44 The former president of ABC News in the United States, Av Westin, discussing the network’s evening programming, held that the audience wants to know one thing more than others, “Is the world safe and am I secure?” Sperry, Sharon L., ‘Television News as Narrative’; in: Adler, Richard E. and Douglass Cater (eds.) _Television as a Cultural Force_. New York: Praeger, 1976, p. 135.

45 Wikipedia (English), ‘News Values,’ Wikipedia. Available at: https://en.wikipedia.org/wiki/News_values#:~:text=The%20news%20value%20of%20a,for%20the%20individual%20or%20group


51 White, 2020, p. vii.


53 Bolt, Betz, and Azari, 2008.


Jessica White found in her literature review on terrorism and the media that: “Mass media reporting can contribute to imitation of terrorism.” See J. White, (2020) op. cit., p. vii. Judith Begeer in her thesis ‘How Media-Reported Violence Spreads: The Contagion of Suicide Terrorism’ (The Hague: Leiden University M.A. Thesis, 2017), found that statistically “….. suicide terrorism spreads via a non-random distribution.” She also concluded that “…..clusters and frequencies in the spread of this type of violence [were] pointing towards contagion.” (Quote from the Abstract).


White 2020 p. 35.

This short list of ethical principles was derived on the basis of responses from editors to author, as quoted in Schmid 1989, p. 546.


Cohen-Almagor, Raphael, ‘Media Coverage of Acts of Terrorism: Troubling Episodes and Suggested Guidelines,’ Canadian Journal of Communication, 30, 2005, pp. 383-409, pp. 401-402. The original set he proposed is larger than the one reproduced here and the sequence of the points he listed has been changed here.

To cite a journalist turned academic, Brigitte Nacos (Columbia University, New York): “Encouraging media guidelines for reporting terrorist incidents may be prudent; however, trusting that news organizations will follow their guidelines is not”. See Nacos 2002, p. 186.

Ibid., p. 388.


74 Hughes, John, ‘Winning the war of words in the campaign against terrorism,’ The Christian Science Monitor, 17 May 2006.
Bibliography


Schmid, Alex P., ‘Frameworks for Conceptualizing Terrorism,’ *Terrorism and Political Violence*, 16(2), Summer 2004, pp. 197-221.


Web-based Resources


Dart Center for Journalism and Trauma, ‘Terrorism’; A Project of Colombia Journalism School. Available at: https://dartcenter.org/topic/terrorism.


Chapter 19
Prevention of (Ab-)Use of the Internet for Terrorist Plotting and Related Purposes

Branislav Todorovic and Darko Trifunovic

The internet has become an indispensable tool for human communication, offering an abundance of information and a great variety of applications. However, the worldwide web also offers ample opportunities for malefactors (e.g., criminals, terrorists, demagogues) to carry out activities cause serious damage. Due to the internet’s wide-reaching nature, any investigation of its (ab)use has to be defined in terms of boundaries. This chapter addresses the (ab)use of the internet for terrorist activities and seeks to provide useful information to detect and address this issue. In doing so, this chapter covers five issues:

● Terrorist group’s employment of social media platforms to recruit new members and communicate with their sympathizers. This chapter explores possible ways to detect, mark, and suppress such activities (e.g., secret encrypted communication, internet deep search software, human-machine interaction, and new generation artificial intelligence tools).

● Terrorist organizations also utilize the internet for propaganda purposes. Based on various examples, this chapter analyses patterns in publications and advertisement of ‘heroic’ terrorist activities, which, in turn, can be useful for anti-terrorist campaigns.

● The internet has proven to be a valuable marketing and public relations medium for terrorism funding purposes.

● Terrorists (ab)use on the internet publicly available information (i.e., by means of data mining) to plan, and carry out attacks. This chapter offers suggestions of measures that can be used for prevention and preparedness.

● Terrorists thrive well on the internet because it anonymously accessible. This chapter explores options and tools for tackling this anonymity (e.g., with the help of behavioral statistics).

The analyzed forms of use/abuse of the internet by terrorists are classified and structured by type and purpose. Possibilities for prevention are discussed for each group or cluster.

Keywords: internet, terrorist activities, prevention, preparedness, propaganda, recruitment.
The title of this chapter might also be “the prevention of the exploitation of the internet for terrorist plotting and related purposes.” In this chapter we will highlight recent developments and limitations of the contemporary methods to prevent and dismantle harmful activities. In addition to this, we will do the following:

- Determine which activities on the internet fall under the category of terrorist plotting and related purposes;
- Create a proper systematization of such activities for further analysis; and
- Provide a comprehensive list of preventive measures.

To begin with, one has to always keep in mind that the (ab)use of the internet for terrorist plotting covers a very broad area, corresponding to the general use of the internet. If a definition of ‘prevention’ would be applied literally (e.g., the one of the Cambridge Dictionary which defines it as “the act of stopping something from happening or of stopping someone from doing something”) that might be understood as being possible to intercept the (ab-) use of the internet by terrorists with a high degree of probability. That, however, is not true in most cases, though it is possible to prevent terrorists from abusing certain features of the internet. In reality, it is more probable that counterterrorism professionals manage to detect and identify terrorist plotting activities that are already underway; they can then prevent these plots from evolving into actual operations, or at least limit some of the possible damage. It might also be possible to prevent further escalation or contagion in the form of copycat acts.

The first to define terrorist activities on the internet. This is a challenging task, as some activities are only partially related to the internet; with the example of so-called cyberterrorism as the most characteristic one. Due to a rapid and broad development of Information Technology (IT) and cyber systems since the early 1990s, cyber security has become a major topic on its own, with cyber attacks and their prevention being just one segment. Therefore, the derived systematization presented below will have to undergo further deliberation and adjustments before reaching its final form.

That the internet provides terrorists with an extensive set of tools is undisputed. For example, the internet assisted Salman Ramadan Abedi in preparing his 2017 Manchester Arena suicide bombing:

“According to the UK Parliament’s Intelligence and Security Committee (ISC), ‘access to extremist material online is reported to have been a key factor in the Manchester Arena attack which killed 22 people’, referring to a newspaper report that the attacker, Salman Abedi, used YouTube videos to learn how to make his explosive device.”

However, the uses of YouTube cannot be curtailed just because someone (ab)used some of its content. Similarly, Google Earth as a tool is assisting a vast number of people on an every-day basis. This is to say that the possibility that terrorists use Google Earth to examine the locations, should not and will not stop Google Earth to operate for the common good (and for the company’s profits).

This raises the question of how to effectively prevent, or at least significantly reduce, internet (ab)use, while maintaining bona fide use. It is often difficult to separate benign and hostile internet users, while also taking into account privacy concerns, and respecting freedom of expression. To cope with the vast amount of information on the internet, there are automatic tools available that can push, remove, or block (access to) content. Occasionally, information is stored unnecessarily on the internet. Without any aspiration to take sides, we present two examples that indicate that these issues need a great deal of attention. Take, for instance, this news report:
“The UK government is trying to restrict access not only to the terrorists’ own channels, but also material hosted on the research website jihadology.net, stating that it is ‘reckless to publish terrorist propaganda online without safeguards to stop those vulnerable to radicalization from seeing it’. As a result, what looks like a double standard has emerged. In February 2015, for example, Fox News in the US broadcasted excerpts of one of the most notorious items of terrorist propaganda ever produced: the last moments of Moaz Al-Kasasbeh, a Jordanian fighter pilot captured by Daesh (also known as the Islamic State of Iraq and Syria, ISIS) who was held in a cage and burned to death. To this day, Fox News continues to host the entire 22-minute video on its website – content which would undoubtedly have been removed by YouTube or Facebook.”

In this particular example, it is worth noting that the academic website jihadology.net was restored after an intervention of scholars who rely on it to study terrorist propaganda materials.

Review: Literature on Terrorist Use of the Internet

Technology is advancing fast in the digital field. Since the late 1980s, the internet has proven to be a highly dynamic vehicle for communication, reaching now more than half of the global population. Technology is also a driving force for terrorist organizations and their supporters for a broad range of objectives. The internet has become a favorite tool for terrorists because of the many advantages it provides, including these: easy access, little or no regulation, weak or no censorship or other forms of governmental control, potentially huge audiences spread across the world; anonymity of communications, fast flow of information, interactivity, inexpensive development and maintenance of a web presence, a multimedia environment, and the ability to influence coverage in the traditional mass media.

Terrorist groups or their front organizations maintain their own websites to spread propaganda, raise funds, recruit and train members, communicate with their followers, and also prepare and sometimes even steer ongoing attacks. They also rely on email, chatrooms, e-groups, forums, virtual message boards, and resources like YouTube, Facebook, and Google Earth.

Fighting online terrorism is complicated and costly. The virtual war between terrorists and counterterrorism forces and agencies is a dynamic one. Rapid developments in technology represent both challenges and tools for global efforts to counter terrorism. While the many benefits of the internet are evident, its downsides are still underestimated when it comes to terrorism. The misuse of internet-based tools for terrorist purposes represents a serious threat, since more and more essential aspects of contemporary society are almost completely dependent on the functioning of computer systems and the internet.

Preventing as well as investigating terrorist use of the internet requires adequate legislation and also effective technical solutions. These challenges differ largely from those identified in the fight against more traditional terrorist activity. As a result of the available network technology and the multitude of internet-based services, these challenges range from addressing the easy availability of instructions on how to commit terrorist acts to monitoring the use of encryption technology in terrorist communications. As terrorist groups turn to technical tools to organize, plan, operate, finance and support their activities, their increasing reliance on technology also makes them more vulnerable to government agencies’ intelligence collection. Governments are developing increasingly sophisticated techniques to identify and track potential terrorists. Rapid advances in technology also permit non-governmental organizations and researchers to detect and monitor many of the online activities of suspected terrorists in cyberspace. Thousands of suspected terrorist websites have been catalogued by various entities around the world. Interlinks between forms of organized crime and terrorism
have been discovered and exposed. Terrorist organizations and organized crime groups often use similar tactics - so much so that that distinguishing between what is a non-political ‘criminal’ and a political ‘terrorist’ act can be a difficult task. On the other hand, many legal and police responses to terrorism parallel approaches to countering organized crime.\(^8\)

The development of increasingly sophisticated technologies has created a network with a truly global reach, and relatively low barriers for entry. Internet technology makes it easy for an individual to communicate with relative anonymity, quickly and effectively across borders, enabling him or her to reach an almost unlimited audience. The benefits of internet technology are numerous, starting with its unique suitability for sharing information and ideas.\(^9\) It must also be recognized, however, that the same technology that facilitates freedom of communication can also be exploited for the purposes of terrorism. The following section explores this in more detail. It is partly based on the findings of a report prepared by the UN Office on Drugs and Crime.\(^10\)

**Methods and Purposes of Internet Use for Terrorist Objectives**

When it comes to terrorist abuses of the internet, it is possible to identify six sometimes overlapping categories: propaganda (including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyber attacks.

1. **Propaganda:** Contemporary propaganda generally takes the form of communications providing ideological explanations, listing grievances and offering justifications for the promotion of terrorist activities. Such propaganda may include textual messages, visual presentations, glossy magazines, religious treatises, audio- and video-music and movie files as well as video games developed by terrorist organizations or their supporters and sympathizers. What constitutes terrorist propaganda - as opposed to legitimate advocacy of a political perspective - is often difficult to determine. In general, propaganda involves the selective and manipulative dissemination of biased information, mixing (half-)truths and lies and appealing in emotional ways to latent widespread prejudices in order to encourage action against political opponents. The promotion of violence is a common theme in terrorism-related propaganda. Terrorist propaganda distributed via the internet covers a range of objectives. It may also be used to showcase the effective execution of terrorist attacks to those who have provided financial support. Other objectives of terrorist propaganda may include the use of psychological manipulation to create a sense of heightened anxiety, fear or panic in a population or subset of it. This may be achieved through the dissemination of disinformation, rumors, threats of violence or images relating to violence.

1.1. **Recruitment:** The internet may be used also as a way to develop relations with, and solicit support from, those held most responsive to targeted propaganda. Terrorist organizations increasingly use propaganda distributed via platforms such as chat groups as a means of clandestine recruitment.\(^11\) The reach of the internet provides terrorist organizations and sympathizers with a global pool of potential recruits. Restricted access cyber forums offer a venue for those initially recruited to learn more about, and provide support to, terrorist organizations and, ultimately, to engage on their own in direct actions in the furtherance of terrorist objectives.\(^12\) Propaganda may be fine-tuned and adapted to account for demographic factors, such as age or gender, as well as social or economic circumstances. Some terrorist organizations have even designed online video games intended to be used as training tools. Such games may lower the threshold of individuals to use violence in real life and promote the use of violence against specific political leaders. Some of these games are offered in multiple languages to appeal to diverse audiences.\(^13\)
1.2. Incitement: The internet provides an abundance of material and opportunities to download, edit and redistribute content that may be considered unlawful glorification of, or provocation to, acts of terrorism. The line between information and influence operations can be a thin one. Media censorship has increased in authoritarian states. However, for democracies governed by the rule of law, restrictions on the exercise of the right to freedom of expression have to be both necessary and proportional to the threat posed. The right to freedom of expression is also linked to other important rights, including the rights to freedom of thought, conscience and religion. Closing down open societies in order to stop incitement to violence by fringe groups in society is not the right answer.

1.3. Radicalization: Incitement, radicalization, and recruitment to terrorism may be viewed as points along a continuum. Radicalization refers primarily to a process of indoctrination that ideologically socializes or converts young people to an extremist worldview and mobilizes them to support, and ultimately perform, acts of violence against designated political opponents. The process of radicalization generally involves the use of propaganda, whether communicated in person or via the internet. The length of time it takes to win recruits depends on the effectiveness of the propaganda and on the mix of individual and social push and pull factors of vulnerable recipients.

2. Financing: Terrorist organizations and supporters also use the internet to raise money for acts of terrorism. They do so in four different ways: direct solicitation, e-commerce, the exploitation of online payment tools and through charitable organizations. Direct solicitation refers to the use of websites, chat groups, mass mailings and targeted communications to request donations from supporters. Websites may also be used as online stores, offering books, audio and video recordings and other items to supporters. Online payment facilities offered through dedicated websites or communications platforms make it easy to transfer funds electronically between parties. Online payment facilities may also be exploited by terrorists through fraudulent means such as identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud. Financial support provided to seemingly legitimate organizations, such as charities, may also be diverted for illicit purposes. Some terrorist organizations have been known to establish shell corporations, disguised as philanthropic undertakings, to solicit online donations. These organizations may claim to support humanitarian goals while in fact much or all of the donations are used to fund acts of terrorism.

3. Training: Since practically all terrorist organizations lack permanent territorial safe havens, many of them have increasingly turned to the internet as a virtual training ground. There is a wide range of media that provide platforms for the dissemination of online training manuals and bomb making information. These platforms are used to share specific methods, techniques or operational knowledge for the purpose of committing acts of terrorism.

4. Planning: Many criminal justice practitioners have indicated that almost every new case of terrorism prosecuted involved the use of internet technology. In particular, planning an act of terrorism typically involves remote communication between several conspirators.

4.1. Preparatory secret communication: The most basic function of the internet is to facilitate instant communication. Terrorists have become increasingly sophisticated at exploiting communications technologies. A simple online e-mail account may be used by terrorists for electronic “dead dropping” of communications. This involves the creation of a draft message, which remains unsent. It leaves minimal electronic traces but may be accessed from any internet terminal worldwide by multiple individuals in possession of the relevant password. There is also an abundance of sophisticated technologies that increase the difficulty of identifying the originator, the recipient or the content of internet
communications. Encryption tools and anonymizing software and steganography are readily available online for download.\textsuperscript{17}

4.2. \textit{Publicly available information}: Organizations and individuals publish extensive amounts of information on the internet. In the case of organizations, this may be a result of a desire to promote their activities and broaden their interactions with consumer in general. Particularly in the age of popular social networking media, such as Facebook, Twitter, YouTube, Flickr and blogging platforms, individuals also publish, voluntarily or inadvertently, an unprecedented amount of potentially sensitive information on the internet, often without considering how it can be used against them.

5. \textbf{Execution}: The use of the internet in furtherance of the operational execution of acts of terrorism offers logistical advantages, while the likelihood of detection and arrest is low as double encryption allows the hiding of the identity of senders and receivers. Internet purchases may facilitate the acquisition of items necessary for the execution of terrorist attacks (e.g., chemicals needed for bomb-making). Stolen credit card information or other forms of compromised electronic payment tools may be used to finance such purchases.

6. \textbf{Cyber attacks}: A cyber attack generally refers to the deliberate exploitation of computer networks as a means to penetrate more or less protected networks. Such attacks are typically intended to disrupt the proper functioning of targeted computer systems, servers or underlying infrastructure, by means of use hacking, viruses, malware or other means.\textsuperscript{18}

Methods to fight cybercrime in general and terrorist use of the internet in particular currently attract a great deal of attention. The reason for this is not just that some of the methods are new and therefore require intensive research, but also that the investigation of crimes involving network technology presents particular difficulties. Effective investigations relating to internet activity rely on a combination of traditional investigative methods, knowledge of the tools available to conduct illicit activity via the internet and the development of practices targeted to identify, apprehend and prosecute the perpetrators of such acts – criminals and terrorists or government agents who are often in another country than where the attack took place. A proactive approach to investigative strategies and supporting specialist tools that capitalize on evolving internet resources enables better identification of data and servers and is likely to yield greater benefits to investigators.

There is a range of specialized utilities and hardware available to investigators with the appropriate technical background and security clearances. Due care should be taken, where possible, in cases involving the acquisition of digital evidence to implement standardized data recovery procedures to promote the retrieval of all the available evidence and the preservation of the integrity of the data source so as to ensure admissibility of evidence in court proceedings. Owing to the fragile nature of digital evidence, its examination is best performed by specially trained forensic experts.

Effective international cooperation is an important factor in many terrorism-related prosecutions. States are legally obliged, under various multilateral and bilateral legal instruments related to terrorism and transnational organized crime, to establish policies and legislative frameworks to facilitate effective international cooperation in the investigation and prosecution of acts of terrorism and serious organized crime. However, there is often a long way to go between legal obligations regarding mutual judicial assistance and the honoring of requests for arrest and extradition of criminals and terrorists abusing the internet in third-party jurisdictions.
Key Aspects of the (Ab-) Use of the internet for Terrorist Plotting

In this chapter we propose a new system for the categorization of the (ab-) use of the internet for terrorist plotting. It is firstly grouped by type (i.e., the method of internet (ab-) use and to which segments of internet it relates) and each derived cluster is further divided by purpose (sub-group). The main purpose is to discuss practical aspects of internet (ab-) use, with an emphasis on prevention. Grouping by type allows exploiting the common denominator among sub-groups within each cluster, which in most cases means that the same or similar preventive & countermeasures can be used for the whole cluster. The classificatory scheme can be used by other analysts by simply reorganizing the sub-groups into new clusters on the basis of selected criteria.

Main Types of internet (Ab-)Use by Terrorists (IAT stands for ‘internet abuse type’)

- **IAT1** - Direct approach over internet (abuse of various means of communication, including mass e-mails, conference calls, etc.) and development of relationships
- **IAT2** - Secret, encrypted, anonymous and similar communications
- **IAT3** - Online multimedia materials
- **IAT4** - Dedicated internet tools; e.g., interactive websites (including specialized ones like e-commerce, undercover NGO or charitable organizations), chat-rooms, etc.
- **IAT5** - Social networking platforms
- **IAT6** - Video games and similar interactive means of promotion, downloadable from internet
- **IAT7** - Online payment tools (including cyber crime techniques)
- **IAT8** - Exploitation of publicly available information & resources
- **IAT9** - Cyber attacks

Division by purpose has been accepted as the following (SG stands for ‘Sub-Group’):

- **SG1** - Propaganda
  - Recruitment
  - Incitement
  - Radicalization
- **SG2** - Financing
- **SG3** - Training
- **SG4** - Planning
- **SG5** - Execution
- **SG6** - Cyber Attacks

General Preventive Measures

An important task is to provides training to staff from law enforcement and corresponding agencies fighting against terrorism. Main tasks can include:

- The detection, recognition and classification of internet-based terrorist activities.
- The use of automatic and semi-automatic tools for identification of internet-based terrorist activities.
- The verification of identified terrorist activities and application of preventive or countermeasures.

Although law enforcement agencies are at the forefront when it comes to the fight against terrorism, it is crucial to establish dialogue and enable cooperation between all relevant
government agencies and departments, as well as with the private sector in order to better prevent the (ab-) use of the internet by terrorist individuals and organizations. This requires all parties to establish in detail a common structure and methodology for fighting against terrorist (ab-) use of the internet.

Another key segment to prevent the (ab-) use of the internet for terrorist plotting is to put in place an adequate legal framework for action. The rule of law requires that the valid evidence is presented; in this case it includes the admissibility of digital evidence in counterterrorism cases in court. Since internet providers are mainly private companies, the issues of securing evidence may also require close cooperation between governmental and private institutions.

The (ab-) use of the internet by terrorists has significant implications for the private sector, in particular for those technology and social media companies whose products and services are used by millions, and these days even billions of people across the globe. While the companies in question have a business incentive to create a digital environment where their users feel safe, internet companies are increasingly compelled by governments to cooperate in blocking, filtering, countering or removing content or accounts based on public safety or national security considerations. In addition, internet users expect the service-providing companies to be transparent, accountable, respect privacy and freedom of opinion and expression, while also ensuring an open, free and secure internet – demands that can be conflicting with each other. Security concerns have led to greater voluntary engagement of the private sector in efforts to respond to terrorist (ab-)use of the internet. This engagement includes industry-driven initiatives and participation in multi-stakeholder and public-private fora focusing on normative, technical and organizational issues, as well as consultation with academic experts. Together, these efforts are hopefully resulting in the gradual emergence of a normative framework shaping private and public action in this area, based on a growing joint awareness of the scope of the problem. However, important challenges remain, including the fact that many industry actors are yet to fully engage while some governmental (over re-) actions can undermine trust in this progress.19

An example of coordinated activities in this area was the first course (2 to 6 July 2018) that was held under the auspices of INTERPOL’s Project Trace, a three-year capacity building program funded by the government of Canada. With a clear focus on detecting, preventing, investigating and ultimately prosecuting terrorism-related crimes, participants learned how to collect, analyze and share information found online. The course was led by INTERPOL experts as well as partners from the International Centre for Political Violence and Terrorism Research (ICPVTR), the Financial and Technology Crime Division of Singapore, the Australian Federal Police, the US Federal Bureau of Investigation (FBI) as well as representatives from Facebook. This was followed by the first INTERPOL-United Nations Office for Counter-Terrorism (UNOCT) workshop on using information collected on social media to target Foreign Terrorist Fighters (FTF). The second session (9-10 July 2018), entitled “Enhancing Member State Capacities to use Social Media to Prevent and Counter the Foreign Terrorist Fighters Phenomenon” was funded by the government of Japan and UNOCT. Through practical exercises, it sought to deepen understanding of the FTF phenomenon via the collection of social media information with the aim to support counterterrorism investigations.20

General Countermeasures

It is very important to understand the motives and purposes of terrorist organizations in order to fight them. In practice, in particular when the (ab-) use of the internet for terrorist plotting is concerned, effective application of countermeasures requires knowledge of the instruments and methods terrorists use to further their goals. In that sense, some segments of the internet and web platforms are better suited for specific Internet Abuse Type (IAT) applications than
others. As the internet develops, and more people learn how to use it, so do terrorists adapt and adjust their (ab-) use of this global communication instrument.

Policymakers, in both government and corporate settings, and the wider counterterrorism policy research community must understand how terrorists use specific platforms in order to effectively prescribe countermeasures. For example, platforms used for content hosting should prioritize mechanisms to identify terrorist propaganda. To achieve this, various techniques for content matching are proving useful. However, some of these techniques will not be as important for platforms used to maintain a group’s community, to communicate securely, and to organize financing. For those platforms, identifying behavioral signals or information-sharing with partners may be more important. Platforms that support numerous functions will need to develop a variety of countering techniques. There is no one-size-fits-all solution to this problem.

21 Penetrating the Deep and the Dark Nets

With the growth of the internet (ab-)use by terrorists has also expanded. Systems that support prevention and counter actions against (ab-) use of the internet by terrorists, have to possess the ability to search, filter, adapt and transfer to its operational databases large amounts of data from the web for further processing – something called data injection. That data needs to be further processed, either by fully automated or by semi-automated tools - a process often called data mining. To achieve investigation objectives, counter-terrorism focused search engines need the capability of handling normal internet data, but should also be able to access data from the so-called deep and dark nets. Specific forms and tools applied for data processing depend on the type of internet (ab-) use by terrorists, as discussed above.

Direct Approach over Internet and Development of Relationships (IAT1)

This type of activity covers communications over the internet in open format (without encryption or attempts to conceal identities of participants). It covers all types of communication over the internet: e-mail; twitter; phone calls and messaging, i.e., voice over IP (VoIP) and instant messaging (IM) (e.g., Viber, WhatsApp, Telegram, WeChat, etc.); Although some of the communication channels claim to be secure by their providers (e.g., Viber or Telegram), they still belong to type IAT1 since there is no assured end-to-end encryption. While the basic encryption might be enough to protect web-based communications by ordinary listeners, it is not enough when hackers, specialists or providers themselves use their tools.

Due to the rather low level of security provided by many internet providers, terrorists and terrorist groups often conduct their communications in codes that do not raise suspicion among third parties. On the one hand that makes their communication more complex, slower and bound to errors, but, on the other hand, it does not draw the immediate attention of human counterterrorism-analysts and/or automatic conversation analysis algorithmic systems. In rare cases where speed is of essence, like when it comes to the execution (Sub-Group 5 or SG5) of terrorist attacks, terrorists might communicate without encryption. By counting on delayed detection and alert mechanisms and inertness among members of response teams, frequently combined with an optimistic view of chances for a fast escape (or, alternatively, a willingness to lose their own lives during the attack), some terrorists take the risk of open communication in the expectation to complete their attack actions and achieve their tactical goal as planned despite a high chance of being detected.

Internet Abuse Type 1 (IAT1) can be used for all subgroups, though in cases of propaganda (SG1) and financing (SG2) it is more often used after initial communication links had already
been established and communication in code was agreed upon. IAT1 is common for active recruitment in cases where direct personal contact does not require covert communication. With regard to recruitment (as part of SG1), type IAT1 is used as a simple and low-cost approach.

Preventive and Countermeasures

Internet Abuse Type 1 (IAT1) is commonly related to covert listening in on conversations or reading of e-mails and messages. While the beginnings of telephone-based mass surveillance dates back more than one hundred years, the situation has changed. Due to the immense number of continuous conversations, these are often captured and recorded and only later analyzed rather than in real time. Contextual search algorithms with machine learning and big data are coping well with traditional IAT1 type. When communication in codes is conducted, machine learning is of great assistance through pattern recognition and other algorithm enhancements. However, by the time intercepted communications are analyzed, the time for actionable preventive measures has in many cases already passed.

Advances made in the field of artificial intelligence, machine learning and big data also raise fundamental legal, ethical and cultural questions as to how these instruments and techniques should be used in counterterrorism. Used appropriately, these technologies are beneficial not only in the fight against cybercrime, but also for scientific research and education. However, at the same time these new tools present greater risks for malicious use and abuses, including by intelligence and security agencies willing and able to invade the privacy of broad sectors of society – more that is warranted by the threat of terrorism.22

Secret, Encrypted, Anonymous and Similar Communications (IAT2)

In order to avoid the use of codes, as in internet Abuse Type 1 (IAT1), and to achieve a much higher general level of security in communications, terrorists and terrorist groups use various methods of secret, encrypting or anonymized communications:

- Secret communications – use of internet capabilities or internet-based software in order to communicate outside of indexed channels, thus avoiding detection and monitoring. One relatively common form is the use of a Virtual Private Network (VPN) - a type of programming that creates a safe and encrypted connection over a less secure network such as the public internet. VPNs operate through the use of shared public infrastructure, while maintaining privacy through security procedures and tunneling protocols whereby the original IP address is exchanged for another, frequently changing, one.

- Encrypted communications – as mentioned in the case of VPN, there are numerous ways and applications that enable communication encryption in some form and with different levels of encryption. Encryption can be applied for voice & video communication (e.g., by scrambling messages) as well as other modes of distant interaction. Encryption software can be easily found and downloaded from the internet.

- Anonymous communications – utilization of internet capabilities to mask the source, location or other parameters of communication which could reveal the identity of persons involved in it. In this case terrorists assume that even if someone monitors the communication, the intercepted information is generally useless since it cannot be linked to specific individuals or terrorist groups. A major drawback of this type of communication is that no names, locations, dates or similar information can appear in
the communication since that may provide clues for revealing the identity of one or more participants in the communication.

Terrorists use various techniques to pass codes for unlocking some forms of communications. In some cases, though, some older and/or simpler methods can be used. Steganography, or the practice of leaving a message hidden in the pixels of pictures, is often overlooked. Such messaging might come in the form of using a predetermined but innocuous code word to send a message or obliquely referencing some shared experience to authenticate true sender identity online. A simple online email account may be used by terrorists for electronic, or virtual, “dead dropping” of communications. This refers to the creation of a draft message, which remains unsent, and therefore leaves a minimal electronic footprint, but which may be accessed from any internet terminal worldwide by multiple individuals with the appropriate password.

IAT2 can be used for all subgroups, providing that clandestine communication form is operational and available to all insider participants in the communication process. However, for financing (SG2) and training (SG3) this type has limited usability – mainly for organizational and consulting segments within the core SG2 & SG3 activities. IAT2 is used for active recruitment, as part of SG1.

Perhaps the easiest way to cope with the (ab-) use of the internet for terrorist plotting within the IAT2 type is to ban and/or restrict the use of clandestine communication techniques for known terrorists or their allies and collaborators. Yet this is easier said than done. Other alternatives might include the use of specialized software for decoding encrypted communications or decrypting them with the assistance of collaborative internet service providers. However, decoding generally requires massive computer power, so again it would be practical to conduct an investigation and restrict decoding and/or decrypting to key suspects in connection with terrorist activities. Furthermore, by tracking the activities of key terrorist suspects it would be possible to spot also steganography, email as well as other forms of anonymous communications.

Brian Fishman, a terrorism expert working for Facebook, suggested a list of questions that technology companies face: How do you determine who is a terrorist? How do you come up with basic content standards? Should companies allow some content from terrorist groups on their platforms in specific circumstances — for instance, in the form of political campaigning by groups like Hezbollah in Lebanon or the Milli Muslim League in Pakistan? : Should some terrorists be completely banned from the platforms no matter what? Should a prohibition extend only to leaders of a terrorist organization or to all known members? How should those categories be defined and what is the evidentiary standard for determining whether someone falls under a category? Moreover, even in the best of circumstances, a company will not be able to create a comprehensive list of the world’s terrorists and enforce their exclusion from the internet. Despite this wider problem, establishing stringent restrictions at the user-level can offer a consistent basis for removing terrorist users from a given platform if the internet company provider becomes aware of them. Yet as long as it is possible to open an account on social media without full proof of identity access to the internet for terrorists cannot be effectively banned.

VPN supplies users with a private internet connection in the sense that the traceable personal IP address of the user is replaced with an alternative IP address from a VPN provider. The result is that the user becomes anonymous in practice during the use of the internet, hidden behind the provider’s IP address. This makes the identification of terrorists as users difficult. Consequently, it is also more difficult to decide in which cases one should initiate a procedure to block or ban a specific use of VPN. Furthermore, activities combating the (ab-) use of the internet by terrorists in this segment concentrates on individual uses of VPN and not on the technology itself, which remains readily available. While there exist certain methods for VPN
blocking, the terms of use of VPN services have not yet been standardized internationally to make this possible across the board.

**Multimedia Materials (IAT3)**

Multimedia materials are placed on the internet with the main goal of propaganda; e.g., advertising terrorists and terrorist groups, disseminating their causes and beliefs, in order to attract new followers and reinforce the determination of existing supporters. Such materials range from simple published messages and texts to music or other files uploaded on various dedicated websites. In addition to video streaming from files, there exists also the capability to broadcast live stream video from a mobile phone, tablet or head-mounted camera. Due to possibilities that terrorist components could be recognized in multimedia materials, often resulting in blocking the access to it or other countermeasures, links to multimedia materials can also be sent directly to specific parties. The main difference with simple communications is that multimedia materials often exist also in multiple languages and can be (re-)used by anyone at any time, thus providing potential access to a broad audience with the aim of audience indoctrination for ideological or other goals. At the same time there is no need for terrorists to be directly involved in the process, unless it is a live broadcast of an ongoing attack.

Multimedia materials can also be used for another purpose – psychological manipulation. In that case, the target is the public at large, with the idea of spreading anxiety and fear, which could enhance the effect of terrorist actions, as well as diminish social cohesion. In those cases, multimedia materials often contain scenes of violence (real or fabricated), in combination with insinuations or subtle suggestions intended to spread disinformation. As a secondary effect it is expected that the initial viewers will spread such rumors and provide further publicity for such materials.

Instructional material available online includes tools to facilitate counter-intelligence and hacking activities and to improve the security of illicit communications and online activity through the use of anonymizing techniques. The interactive nature of internet platforms allows the building of a sense of community among individuals from different geographical locations and backgrounds, encouraging the creation of networks for the exchange of instructional and tactical materials. IAT3 can be efficiently utilized mainly for subgroups SG1, SG2 and SG3. For instance, as part of SG1, passive recruitment occurs when terrorist organizations recruit individuals through indirect means, such as addressing groups of people through media campaigns and recruitment materials with the intention of familiarizing them with the aims and activities of the terrorist organization.

Driven by business, user and government prerogatives, major technology and social media companies are investing significant resources into developing measures to respond to terrorist use of their products and services. These efforts are largely approached from a content management perspective and include:

- Adapting terms of service (TOS) and community guidelines to prohibit certain content, activity and forms of behavior. In general, most major internet companies have a zero-tolerance policy for terrorist content and activity on their platforms and have committed themselves to ensuring the safety of their users. In light of the challenges in determining who terrorist actors actually are, some companies use international, regional or national sanctions lists to guide their policies on this issue.
- Developing guidance and systems (human and automated) for content flagging, referral and content/ account removal and for remedial action.
- Establishing guidance and systems for responding to law enforcement and government content/ account removal or data access requests.
- Establishing transparency measures for government requests.
- Establishing, training and sustaining content policy and legal teams.
• Cooperating with government or regional Internet Referral Units (IRUs), when required.
• Developing tools and mechanisms (both human and automated) to counter the narratives of terrorist and violent extremist groups and their followers, carried out in conjunction with government agencies and/or civil society and community organizations.28

As mentioned before, artificial intelligence, machine learning and big data allow some degree of control of multimedia materials on the internet. Identified content that is related to terrorism and terrorist activities can lead to removal and subsequent ban of related multimedia materials. It is known that terrorists use code words to avoid immediate detection, but artificial intelligence and machine learning provide their opponents with the ability to perform in-depth content analysis which can overcome masking attempts. However, there are several potential obstacles for the efficient application of such technologies. The first one is the legal aspect: can such activities be made mandatory to internet providers, or should it be left to private companies to decide when and how to act, in particular in cases when the content in question is ambiguous? YouTube has a policy for “borderline” content that technically does not violate the company’s terms of service: the content can stay online, but it is demonetized (i.e., not linked to advertisements) and not recommended to viewers.29 Other potential obstacles for application of state-of-the-art technologies are costs considerations for the internet providers themselves.

**Dedicated internet Tools (IAT4)**

Dedicated internet tools; e.g., interactive websites, chat-rooms, forums, etc. Though slightly outdated and replaced in many cases by social networking platforms, standard internet tools remain in use due to limited security. Internet users can create a website and declare its purpose (true or false) without the need to present any positive identification. The (ab-) use of IAT4 type on the internet for terrorist plotting often involves some level of access restriction such as password protected websites, restricted access to chat-rooms, etc. In cases where websites operate like online stores (e-commerce), selling various items to supporters like books, such websites have to include some form of online payment instrument - which places these in type IAT7.

It is important to distinguish the role of charitable front organizations in IAT4 from their role in IAT7. In IAT4, charities are analyzed regarding their organizational form; i.e., as shells that utilize certain mechanisms to connect and motivate people to get involved in specific activities aiming to achieve predefined goals. Within those activities, more or less openly and on a case-by-case basis, persons are approached with ideological propaganda or radicalizing concepts which can lead to terrorism. The aim is to create bonds with participants in charitable organizations, to get to know them and gain their trust, in order to convert them to become followers. IAT7 type is dealing with the more specific role of charities and certain non-governmental organizations in fundraising. IAT4 is mainly used for subgroups SG1, SG2 and SG3.

Measures used for IAT4 type are based on similar methodologies, software and algorithms as for IAT3, but with a greater focus and finer optimization for web-based contextual searches.

**Social Networking Platforms (IAT5)**

Social networking platforms differ from other internet tools in the sense that they connect the user (individuals, institutions or other entities), often represented by the user’s profile, to other
individuals or groups with the goal of inducing them to exchange opinions, views and all types of information commonly found in social gatherings. The (ab-) use of social networking platforms on the internet for terrorist plotting is usually tolerated by references to the right of freedom of speech, and thus the right to present alternative viewpoints. However, it constitutes an abuse of the freedom of expression to spread violence-oriented propaganda. Unfortunately, there is a broad grey zone existing between two completely opposite issues: the peaceful exchange of ideas, and the glorification of violence. Admittedly, it is not always easy to conclude with certainty whether some online discussion is simply conversation, and when it is hateful propaganda. Furthermore, to block, ban or shut down some specific communication on social networking platforms often requires that some legal procedures have to be initiated which requires that malicious intent has to be proven.

Social networking platforms can also be used for psychological manipulation, as mentioned under IAT3. Social platforms are particularly useful for terrorists for finding potential recruits among vulnerable members of certain social groups. In the case of IAT5, the capability to exchange information and views through social networks offers a framework for the distribution of (dis-)information for terrorists. The objectives are similar with IST3: the creation of anxiety and fear, the undermining of social cohesion and the spreading of false rumors. IAT5 is mainly used for subgroups SG1, SG3 and SG4, although it can also be useful for terrorists during the preparatory phases of attacks (SG5).

Most advanced techniques for detecting terrorist related materials within social networking platforms involve entity recognition and state-of-the-art text analytics in a large body of social media content. Mathematical models together with adequate metaheuristic methods have been designed to provide efficient search mechanisms in social networks with large numbers of users. The designed models and metaheuristics can be used as additional big data analytic tools as follows: they may be combined with existing software for collecting data from the web or for use in already existing professional databases, or they can be used in combination with existing clustering and data mining techniques to improve search quality. There exist also context search algorithms that allow analysis of coverage in multiple languages. However, despite the application of machine learning, fully automatic running of such tools still requires improvements in existing software.

Undoubtedly, some practices - notably restricting content, account removal, providing access to user data for government agencies, or engaging in online social engineering practices - continue to raise important ethical and legal issues.30

The question whether or not governments should require tech companies to conduct counter-terrorism operations is politically charged. However, the voluntary efforts made by some of the major internet companies are likely to have a far greater impact on addressing the problem of terrorist exploitation of the internet. For example, in the first nine months of 2018, Facebook removed 14.3 million pieces of content related to the Islamic State, al-Qaeda, and their affiliates, only 41,000 of these items were flagged by external sources, primarily regular users. The overwhelming majority of the content removed was the result of Facebook’s voluntary internal efforts.31

By raising the awareness of people, it is possible to improve the reporting of offensive content which is terrorism- or extremism-oriented. Early reporting by users of social networking platforms, despite the advances in automatic detection procedures, continues to be an effective way to reduce terrorist (ab-) use of this segment of the internet. In turn, experiences gained from the analysis of user’s reporting can be used to improve the operation of automatic detection algorithms and contribute to faster takedown responses.

Online discussions provide an opportunity to present opposing viewpoints or to engage in constructive debate, which may have the effect of discouraging some potential supporters. Counter-narratives with a strong factual foundation may be conveyed through online discussion forums, images and videos. Successful messages may also demonstrate empathy.
with the underlying issues that contribute to radicalization, such as dire political and social conditions, and highlight alternatives to violent means of achieving desired outcomes. Strategic communications that provide counter-narratives to terrorist propaganda may also be disseminated via the internet in multiple languages, to reach a broad, geographically diverse audience.32

Social media platforms often define terrorism and extremism in their own way. Facebook’s original definition of terrorism, for example, was “any non-governmental organization that engages in premeditated acts of violence against persons or property to intimidate civilian, population, government, or international organization in order to achieve a political, religious, or ideological aim.”33 This definition was subsequently modified to focus its application to terrorist organizations. However, we know that terrorist groups often draw on ideas developed by extremist organizations. Extremism – both violent and non-violent – can lead to terrorism.

Therefore, to stop social media platforms being used by extremists and terrorists, technology companies might wish to take the following steps. First, they should create new “extremism” or “terrorism” categories within their existing reporting systems. This would allow users of their platforms – including the public, or people known to terrorists who are concerned about the material shared with them – to report and flag such materials. On YouTube, users can flag a video uploaded by a member of the public as “violent or repulsive” or as “promoting terrorism” or as “hateful or abusive content,” but not all three. The overlapping nature of this material needs to be acknowledged by allowing multiple flags. Second, a better and more consistent appeal process and feedback mechanism should be created. This is particularly important for material that is not taken down from these platforms. Users should be able to have a conversation with decision makers, and decisions should be explained thoroughly and transparently, breaking down why some material is allowed to remain on the platform, and other online material is removed. While some companies publish quarterly reports or blog posts on this issue, we need to move beyond metrics to specific case studies and aim for more open conversations between consumers and social media companies.34 Good examples of reports that provide relevant information on tools and policies are “Hard Questions: What Are We Doing to Stay Ahead of Terrorists?”35 and “Combating Hate and Extremism” – both by Facebook.36

In many countries, recruitment into terrorist organizations occurs not only through direct social contacts but also on online platforms. Regarding the latter: one opportunity for operational intelligence and security agencies is to work more closely with social media and internet and web-hosting providers. Where content promoting terrorism or facilitating recruitment activities is found, financial investigations should be initiated to determine who controls and finances suspect accounts. While in some cases no financing may be involved, some of the case studies indicate that professionals have been hired to develop a platform to spread terrorist material.37

**Video Games and Similar Interactive Means of Promotion (IAT6)**

This type of (ab-) use of internet activities is related to interactive means of promotion, downloadable from the internet. Providers range from file-sharing sites to cloud repositories. The difference with dedicated internet tools (IAT4) is that IAT6 assumes that interactive promotion is only delivered (downloaded) over the internet and subsequently used offline or as a local installation with an internet connection. Typical examples would be video games (which can also be used for training purposes), interactive learning systems, magazines and brochures in digital form for downloading and offline browsing. These are often available in multiple languages to increase audiences and impact. IAT6 is very difficult to combat since the downloaded promotion materials are no longer “visible” on the internet. Therefore, even when some content is banned or blocked at a specific web location, it can still circulate by
direct coping or reappear at new locations, possibly published by another terrorist member, supporter or sympathizer who has downloaded it in the first instance.

Some uses of the internet and of internet communication technologies (ICT) for terrorist purposes are often indistinguishable from regular use of the internet by ordinary users or groups, making it very difficult to address the issue. Calls by governments at the international, regional and national levels to take “urgent action” against online extremism or terrorist use of the internet are growing, notably in terms of restricting online content with the aim of protecting public safety. Such calls to action tend to be directed against intermediaries (i.e., internet service providers, technology enterprises and social media companies) rather than the actual creators of the content. This is often due to the fact that creators of terrorist content operate out of foreign jurisdictions or places, where law enforcement is weak. There are competing arguments as to the merits of various approaches. On the one hand, these are often perceived as enhancing public safety and protecting the vulnerable. On the other, some hold that interventions violate the human rights of users, and undermine trust in companies as well as in government. In short, much needs to be done by all parties to ensure a more appropriate balance between offline prevention and online counter measures and in demonstrating convincingly what methods yield effective results.38

It is important to emphasize the distinction between mere propaganda and material intended to incite acts of terrorism. In some national jurisdictions, in order to be held liable for incitement to terrorism, a showing of the requisite intent and a direct causal link between alleged propaganda and an actual plot or execution of a terrorist act is required. For example, in a contribution to an expert group meeting, a French expert indicated that the dissemination of instructive materials on explosives would not be considered a violation of French law unless the communication contained information specifying that the material was shared in furtherance of a terrorist purpose.39

**Online Payment Tools (IAT7)**

In contrast to simple and low-cost approaches to general online recruitment, referred to above, terrorist organizations are often spending considerable amounts of money on recruitment networks and on expenses related to gathering and “processing” recruits. Quite often new recruits have to move to specific locations (requiring fake identities, travel and accommodation expenses), and in such cases there is also often remuneration involved (not unlike payments to mercenaries). Recruitment networks frequently use premises of registered or unregistered religious organizations, places of worship or similar locations as assembly points. Sometimes premises have to be rented. Even more expenses have to be incurred for the preparation and execution of terrorist acts. In order to finance all this, terrorist organizations have to collect and transfer amounts of money to specific locations.

Online payment systems are basically used for transfer of funds from different sources to accounts belonging to, or handled by, terrorist organizations (e.g., in the case of shell companies) or funds are transferred to designated individuals (frequent using false or masked identities). Funds might have various origins, starting from direct solicitation, illegal businesses and money laundering, through transfer of cash collected by hand by associates. Yet, funds can also be obtained from legal business or might include legitimate donations. There are also possibilities of engaging hackers, belonging to, or associated with terrorists, to perform phishing, hacking or similar activities that involve transfer of stolen money to terrorists’ accounts. In general, the internet offers a number of advantages that are of interest to terrorists. To mention just a few: global coverage and reach, technological advance in commerce on the international level with commonly accepted ways of handling electronic transfers of funds (including online banking, mobile phone banking, etc.) and the use of legitimate ways to collect money for terrorist needs (e.g., gambling, crowd-sourcing, e-
commerce, virtual sales, etc.). In contrast to online criminal activities involving terrorists, which are the target of international police investigations on a daily basis, the activities of charities and nongovernmental organizations (NGOs) are much more problematic to control. It is very difficult to distinguish charities and NGOs with legitimate goals from those which are meant to finance acts of terrorism, in particular when the cause is masked with false pretenses, or when charities and NGO are infiltrated by terrorists who deflect part of the income for their own nefarious purposes.

In the Eurasian region, recruitment often occurs through religious organizations and in a number of cases the majority of the members of terrorist organizations are recruited by established recruitment networks which require financial support. In addition, maintaining a digital magazine and keeping IT teams engaged requires a continuous funding stream. Although the access and use of social networks and the creation of websites is low-cost and can even be free of charge, some terrorist organizations create high-quality content, which tends to require the involvement of experts and the use of sophisticated equipment. Due to the scale and variety of forms of distribution of this type of content, it is likely that a number of bloggers and moderators are participating in the distribution of the material. There are opportunities for strengthened co-operation between the key operational authorities within national counterterrorism/counter-financing of terrorism (CT/CFT) frameworks, particularly the units in charge of terrorist financing investigations and those involved in the collection of intelligence data on recruiting activities. Often, these functions are performed by different investigative entities which operate in separate spheres which can make the detection of recruitment financing activities more challenging. CT-professional should take note of FATF’s (Financial Action Task Force) work on interagency CT/CFT information sharing which offers good practices as well as practical tools.40 IAT7 can be efficiently utilized mainly for subgroups SG2 and SG5.

There is widespread agreement at this point among governments that the internet has created serious counterterrorism vulnerabilities and that action is needed to counter this growing threat. There is far less agreement, however, on what concrete steps can and need to be taken. The US government has taken a number of unilateral aggressive actions in this area, specifically designed to address the abuse of the internet for terrorist financing purposes. This has included a number of prosecutions of suspected terrorists for their internet-related activities. The US has also used its law enforcement tools more broadly, targeting money remitters without adequate internal anti-money laundering/counter terrorist financing compliance systems. Not all countries have been as proactive as the US on this front. First, many countries lack the technical capabilities necessary to investigate online terrorist activity. Second, there is still a debate about how far governments should go in cracking down on some internet-related activities. Some governments are concerned that taking drastic steps will curtail the right to freedom of expression. There is also an active debate about what works best from a counterterrorism perspective – particularly whether it is more valuable to monitor terrorists’ activities on the internet for intelligence purposes, or to shut their websites down. Third, the laws in this area have not kept up with the technological changes, and there is no international agreement about what changes should be made to move forward. Some of the actions of the United States are a step in the right direction, but without broader international cooperation on this issue, there are limits to what can be accomplished.41

Exploitation of Publicly Available Information & Resources (IAT8)

This type of (ab-) used internet activities is covering a very broad area. Therefore, it is quite difficult to provide extensive coverage of all possible cases. Some examples might include Google, Instagram, Facebook, Wikipedia, etc. – in essence any public internet source that provides information useful for specific terrorist purposes and objectives.
Organizations and individuals often publish large amounts of information on the internet. In the case of organizations, this may be a result of a desire to promote their activities and encourage interactions with customers and the public in general. Some sensitive information that may be used by terrorists for illicit purposes is also made available through internet search engines, which may catalogue and retrieve inadequately protected information from millions of websites. Furthermore, online access to detailed logistical information, such as real-time closed-circuit television footage (CCTV), and applications such as Google Earth, which is intended for, and primarily used by, the public for legitimate ends, may be misused by those intent on benefiting from the free access to high-resolution satellite imagery, maps and information on terrain and buildings for the reconnaissance of potential targets from a remote computer terminal.42

Particular risks may ensue when terrorists gather information related to critical infrastructures, which allow them to discover vulnerabilities and facilitate more precise targeting. Ranging from airports and other transportation related infrastructure to power- and water- supply systems which are vital for society (including nuclear power plants), serious damage to critical infrastructure can result in both direct and indirect damage, including loss of lives. For this reason, the segments of the (ab-) use of the internet for terrorist plotting and related purposes that overlap with Critical Infrastructure Protection (CIP) and resilience activities should be merged and handled as a coordinated activity.43

Militants use online mapping tools to plan attacks, monitor news, and identify potential recruits. Various platforms can be used for these purposes, including social media, traditional media, search engines, and specialized tools for identifying sensitive targets. These are the same tools that are used by ordinary folks to find grocery stores, reconnect to old friends, and search for the quickest ways to get from A to B.44 However, in fact these are also dual use tools that can be abused by terrorists.

IAT8 is mainly used for subgroups SG4 (e.g., intelligence gathering) and SG5, with emphasis on the latter. Due to the abundance of information on the internet, IAT8 might also be used for other subgroups, depending on the specific terrorist’s plans and goals.

Unfortunately, this type of instrument requires the most painstaking efforts to counteract. There is no tool on the internet for direct analysis and recognition, either by humans or by automated systems that can tell when open sources are used for good or evil. Only by following globally the activities of terrorists and their supporters on the internet might it become possible to guess with some degree of confidence their motivation and target selection. The effectiveness of such actions would have to be based on several assumptions: that the terrorists are known, that their web-based activities are monitored, that it is possible to find a behavioral pattern within their internet searches that can indicate specific terrorist aims and, finally, that there is enough evidence for taking preemptive legal or operational action.

It would be much more productive to conduct surveillance of web-based activities of known or suspected terrorists once there are indicators of terrorist plotting from other IAT categories. In that case such indicators could identify behavioral patterns that could guide the search for the proverbial needle in the haystack. However, the issue of use of gathered data as evidence in court for any legal action remains to be solved.

Cyberattacks (IAT9)

Cyberattacks represent a category of its own, since the impact and expansion of such attacks are related to the general growth of cyber systems. The preparation for cyberattacks involves various other, already discussed above, internet activities like communication, propaganda, fund raising, recruitment, etc. (i.e., from SG1 to SG5). Therefore, cyberattacks are mentioned here for reference purposes only, because strictly speaking as a type they are also part of internet activities (ab-) used by terrorists.
In recent years, there has come into existence a whole new discipline named Cyber Protection. It studies cyberattacks and designs counter-measures. Due to the complexity of the problem, to prevent and combat cyberattacks, cyber protection requires a range of national and cross-border efforts.

There is an urgent need to develop an international game plan in order to combat cyberattacks by terrorists. To this end, an 8-step global counter cyber-terrorism game plan has been proposed:45

- **Step 1**: Reaching a common definition of terrorism and cyber terrorism is the starting point. Which activities on the internet (e.g., hacking, propaganda, attacking to infrastructures etc.) should be counted as cyber terrorism must be defined exactly. Speaking the same language and creating a common technical language should be the starting point.
- **Step 2**: Essential national and international legal measures have to be taken. International legal arrangements must be put in place. Accordingly, national legislation has to be harmonized with international treaty obligations.
- **Step 3**: Both bilateral and multilateral agreements on cyber security cooperation must be signed, ratified and implemented between countries.
- **Step 4**: An intelligence pool (e.g., in the form of fusion centers) needs to be created in order to collect and share intelligence simultaneously in real time between participating countries. Collecting intelligence should include not only monitoring terrorist websites but also collecting electronic evidence about plots to engage in cyberattacks.
- **Step 5**: Cyber defense expert teams ought to be created and put in charge to act internationally whenever a country encounters a cyberattack. The number of quick national response teams ought to be increased, e.g., with the help of NATO’s Computer Incident Response Capability and the Estonia-based Cooperative Cyber Defense Centre of Excellence. An international cyberattack response training program should be established.
- **Step 6**: International counter-cyberattack exercises should be planned and executed in order to help participating governments to demonstrate and share their proficiency and experience.
- **Step 7**: A well-organized international decision-making process that spans from detection to neutralization (or disruption) of cyberattacks should be formed. Internationally authorized executives should respond to any attack affecting international security, based on pre-agreed rules of engagement.
- **Step 8**: After-reaction analyses should be conducted in order to identify and improve weaknesses in the defense process. A feedback, ‘lessons learned’ mechanism should be put in place in order to improve reaction for the next attack.

**Conclusion**

Preventing terrorists from (ab-)using the internet is in many ways a Sisyphean task. The more the society and specialized agencies develop and apply measures to counteract terrorists, the more terrorists are likely to adapt and find new ways to exploit the internet for their purposes. However, the situation is not hopeless, and one should not reduce efforts to counter abuse. One should not be intimidated into accepting the continued existence of terrorism and its expansion online which, at least in part, is due to the mixed blessings of the internet.

This chapter systematic analysis of uses and abuses of the internet for terrorist plotting and related purposes can serve as a good starting point for non-experts to understand the basic tools and methods that terrorists use. That should help to enhance the capability of governments and
societies to react to terrorist propaganda. With greater public awareness of terrorists’ online activities, attentive ordinary users of the internet can, in fact, become part of an early warning system for the prevention of internet abuse by extremists and terrorists.

The analyzed prevention methods and the counter-measures suggested against the (ab-) use of the internet for terrorist plotting and related purposes should also be of use for professionals who are involved in counter-terrorism. While experts on terrorism from law enforcement and from intelligence agencies certainly know more details about terrorists’ modus operandi, they often lack a hands-on experience on how IT providers operate on day-to-day basis. On the other hand, web service providers, websites hosts and other specialized private IT sector stakeholders are usually more focused on general continuity of service issues than on possible terrorist abuse of their instruments and technologies. As has been emphasized repeatedly in this chapter, there is a need for close cooperation and improved public-private partnerships between all state and civil society stakeholders when it comes to preventing the mis- and abuse of the world wide web and the internet. As creators of the new system for the categorization of (ab-) uses of the internet for terrorist plotting presented in the preceding pages, we hope that this classification will assist others in more effectively combating terrorist (ab-) uses of the internet.

Dr. Branislav Todorovic is a member of the Institute for National and International Security (INIS), Serbia, and a Senior Research Associate in NTUA – National Technical University of Athens and AUA – Agricultural University of Athens, Greece. He also cooperates since 1989 with MASBG – Faculty of Mechanical Engineering, University of Belgrade, Serbia. He is a full member of the Technical Chamber of Greece (TEE) and the Technical Chamber of Serbia. Branislav Todorovic has participated in many commercial and R&D projects, and produced international conference papers. His background covers 30 years of work in environmental sciences, energy and water topics, Critical Infrastructure Protection (CIP), cyber security and IT/ICT, especially GIS, CAD, programming & software development, 3D modelling, databases, etc. He has worked in multidisciplinary projects related to capacity building, public participation, energy and water resources management, renewable resources, modelling of processes, Decision Support Systems (DSS), expert systems, and complex designs.

Dr. Darko Trifunovic is a Senior Research Fellow and lecturer at the Faculty of Security Studies of the University of Belgrade and a Senior Adviser at the Research Institute for European and American Studies in Athens, Greece. He is also a guest professor at FUDAN University – Center of American Studies, Shanghai, China. Dr. Trifunovic is a specialist in Security Studies, Intelligence & Counter Intelligence Studies as well as Counter-Terrorism, National and International Security Studies. He is a former diplomat (First Secretary of the Foreign Service of BiH at the UN). Dr. Trifunovic is the representative for Serbia and Montenegro in the International Strategic Studies Association (ISSA). He is a member of the Advisory Board of the Institute of Transnational Studies, Munich, Germany. Dr Trifunovic is regular speaker at the International Counter Terrorism Institute, Tel Aviv, Israel, and one of the founding Members of the International Counter Terrorism Academic Community (ICTAC). He has published a number of academic books, papers and articles.
Endnotes

2 Cf. Cambridge University Press, official website; Available at: https://dictionary.cambridge.org/
3 A secondary critical issue in relation to this topic, is the possible misuse of the information presented in the following pages. However, this chapter will present mainly publicly known methods for the prevention of the (ab-) use of the internet by terrorists. It is up to the professional CT reader, in case there is a need, to get in touch with institutions or projects dealing actively with the issue under consideration for more detailed and operational useful information.
5 Idem.
8 Coninss, Michèle, ‘Responding to terrorist use of the internet’ (2019), Global Initiative, p. 1; Available at: https://globalinitiative.net/terrorist_use_internet/.
9 See, for example, International Covenant on Civil and Political Rights (General Assembly resolution 2200 A (XXI), annex), art. 19, para. 2.
13 Weimann, Gabriel, ‘Online terrorists prey on the vulnerable’, Yale Global Online, 5 March 2008; Available at: www.yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable.
18 Pursuant to the International Telecommunication Union Toolkit for Cybercrime Legislation, section 1 (n), malware may be defined as a program that is inserted into a computer program or system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the computer program, data or system.


UNODC (2012), op. cit. p. 8


Kavanagh, Camino et al, op. cit., p. 5.

Owen, Laura H., op. cit.

Kavanagh, Camino et al, op. cit., p. 6.

Fishman, Brian, op. cit., p.83.

UNODC (2012), op. cit.

Facebook, Community Standards, Part 2: Dangerous Individuals and Organizations, 2020; Available at: https://www.facebook.com/communitystandards/dangerous_individuals_organizations


Facebook, Combating Hate and Extremism, 2019; Available at: https://about.fb.com/news/2019/09/combating-hate-and-extremism/

FATF, op. cit.

Kavanagh, Camino et al, op. cit. p.5

UNODC (2012), op. cit.

FATF, op. cit.p.25.


UNODC (2012), op. cit.

See for more on this: Todorovic, Branislav et al, Chapter 22 - Contribution to Enhancement of Critical Infrastructure Resilience in Serbia, Resilience and Risk - Methods and Application in Environment, Cyber and Social Domains, Proceedings of the NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructure Safeguarding, Azores, Portugal, 26–29 June 2016, pp 531-551.

Fishman, Brian, op. cit.

Bibliography


International Covenant on Civil and Political Rights (General Assembly resolution 2200 A (XXI), annex), art. 19, para. 2.


Web-based Resources


Facebook, *Combating Hate and Extremism*, 2019; Available at: https://about.fb.com/news/2019/09/combating-hate-and-extremism/

Facebook, *Community Standards, Part 2: Dangerous Individuals and Organizations*, 2020; Available at: https://www.facebook.com/communitystandards/dangerous_individuals_organizations


Malik, Nikita, ‘The Fight Against Terrorism Online: Here’s The Verdict’, *Cybersecurity, Forbes* (2018); Available at: https://www.forbes.com/sites/nikitamalik/2018/09/20/the-fight-against-terrorism-online-heres-the-verdict/#70a0cf814dc5

Owen, Laura H., “Terrorists use the internet in much the same way as other people. How should tech companies deal with it?,” NiemanLab, Cambridge, Mass.: Nieman Foundation, Harvard University, (2019); Available at: https://www.niemanlab.org/2019/04/terrorists-use-the-internet-in-much-the-same-way-as-other-people-how-should-tech-companies-deal-with-it/
Chapter 20

The Role of Intelligence in the Prevention of Terrorism
(Early Warning – Early Response)

Kenneth A. Duncan

This chapter outlines how intelligence has adapted to the ever-changing threat of terrorism, and the crucial role “warning” has played and will continue to play in countering and mitigating this threat. To better understand warning’s capabilities and limitations, it also explores the nature of intelligence as well as the factors underlying warning’s collection, analysis, production, dissemination, and reception. It traces the relationship between intelligence and law enforcement agencies as it evolved as part of the US government’s organizational response to terrorism from the late 1960s onward, highlighting both its strengths and weaknesses. Finally, it discusses problems arising from the often-troubled relationship between intelligence producers and consumers – from policymakers to the general public – which can lead to obstacles in turning an early warning into an early response.

Keywords: 9/11, early warning, homeland security, intelligence, prevention, public warning, TIPOFF, United States.
“The terrorism threat is constantly evolving in response to social, political, and technological change, as well as adapting in response to counterterrorism pressure.”

- Daniel Byman

**Introduction: Understanding Intelligence**

At the main entrance to CIA’s headquarters building in Langley, Virginia is an inscription from the Gospel of St. John: “The truth shall make you free,” which reflects Intelligence Officers’ belief that their role is to “speak truth to power.”

But contrary to this common view regarding intelligence assessments, nothing could be further from the truth. Intelligence and warning are not about objective truth at all. Instead, they are about probability, or as former CIA Director Michael Hayden put it, “If it is a fact, it ain’t intelligence.”

Precise information such as that obtained in 2010 about bombs concealed in photocopier cartridges airmailed by Al-Qaeda in the Arab Peninsula (AQAP) is rare and is not a warning at all, but actionable intelligence. To obtain it, an intelligence service or police department has to be, not only competent, but also lucky. Intelligence-derived warning is about assessing the threat potential of various terrorist groups and, more recently, often of individual terrorists and proto-terrorists. In this respect, it resembles the intelligence community’s (IC’s) role in producing indications and warning (I&W) during the Cold War to warn of evolving military threats.

There is a basic difference between the two, however. Terrorist threat warning is the mirror image of I&W. During the Cold War, both NATO and the Soviet Union were better at assessing each other’s respective military capabilities than they were at understanding their opponent’s intentions. To illustrate this, in the early 1980s, the Soviet Union misinterpreted President Reagan’s ‘Evil Empire’ rhetoric as preparatory to a nuclear attack.

In contrast, terrorists are not reluctant to share their general intentions to attack us - their numerous threats by audio, video, and internet leave us in no doubt about that. What we are less well informed about is the relationship between their intentions and capabilities to carry out specific attacks. When Al-Shabaab, a Somali-based terrorist group, produced a video calling for attacks on Oxford Street shops in the UK and the Mall of the Americas in the US (among other targets), they were “publicly calling for independent actors in their homelands to carry out attacks,” but they were not believed to be capable of sending their own terrorists.

No one knew who was listening or motivated by this.

In intelligence parlance, terrorism is a hard target. It is one of those awkward issues – international organized crime and the proliferation of weapons of mass destruction are others – that are not and never were problems exclusively for intelligence or for law enforcement or for diplomacy, or for the military for that matter. Unlike military forces, terrorists do not have armored divisions, intercontinental ballistic missiles, an air force or navy, which negates much of the IC’s capabilities, themselves legacies of the Cold War. Satellite images, for example, of a vehicle loaded with explosives looks like all the others on the streets of Baghdad, Kabul, Cairo or anywhere else in the world.

Terrorist units are usually small and often comprise nothing more than a group of friends or even a single individual who self-radicalized - the increasingly common lone-actor phenomenon. Incidentally, both former US and Soviet intelligence officers agree that most spies self-present themselves to intelligence services; they are volunteers and have not been recruited. Terrorists are less likely to turn on their colleagues due to their high level of
commitment and close connections to other cell members. This new generation of terrorists may not have any meaningful direct connections with any known groups, which makes detection of these smaller groups even more difficult.

**Warning: Its Nature, Role, and Mechanics**

Warning begins with intelligence, which is usually secret and, therefore, not available to anyone without ‘need to know’ and proper security clearances. After all, why would anyone declare something ‘secret’ if they wanted to share it indiscriminately? In large measure the IC commonly classifies intelligence, that is, declares it to be secret and restricts access to it, in order to protect its method of acquisition – known in the trade as “sources and methods.”

The important point to remember about protection of sources and methods is that it is not a reflection of the veracity of the intelligence. To classify intelligence as “Top Secret” is not a declaration that it is twice as reliable as Secret intelligence. Secret Intelligence, in turn, is not necessarily more reliable than public statements or other open-source material, such as news reports. The chief of the intelligence service of a foreign country might tell the CIA in confidence about corruption in his government or he might make an open declaration of it in a local newspaper. His information might be true or false but one cannot judge that by its intelligence classification. This was not such a problem during the Cold War when the universe of those involved was relatively limited. To return to the example of satellite imagery: apart from photos of ubiquitous cars and trucks, military hardware is often hard to disguise. Soviet jet fighters, for example, were usually shipped disassembled in crates and since each type of aircraft had its own unique crate, analysis of a crate’s image (“crateology” as it was called) revealed which type of fighter aircraft it contained. Furthermore, finished intelligence of this nature, when disseminated to key military, intelligence, and policy customers, was comprehensible for its consumers because all understood the reliability of the technical intelligence and its limitations with regard to guessing the underlying intent.

Consider what happens with terrorism intelligence when those with “need to know” includes the broader domain of homeland security: law enforcement, crisis management, crisis response, border security, and regulatory agencies. It goes still further into the universe that lies outside the US Federal Government, such as state and local health officials, state and local police, private corporations, and increasingly the general public, few of whom are able to see secret information or are used to understanding the nuances of intelligence products. New customers require new forms of information, ranging from guidance on potential threats to critical infrastructure, to terrorist names and identifying data for watchlists. As it is not possible to share everything with everyone, effective sharing requires a new paradigm in order to ensure that everyone has access to the information necessary to perform their duties.

This brings us to the often-overlooked, yet critical element in intelligence preparation: analysis. As noted above, intelligence, especially warning, begins where the truth leaves off. The analyst’s role is to transform raw intelligence, including verified information, such as the movement of terrorists or transfer of their funds, into finished intelligence and warning products. In doing so, it provides insight into, and possibly understanding of, an event, a situation, or the intentions and/or capabilities of an adversary, but this is not the same thing as the truth. In the words of one of CIA’s veteran analysts:

“The business of intelligence analysts is more about putting facts in perspective. … Sources – clandestine, open source, technical, diplomatic etc. – are not the same as knowledge. Sources are not the equivalent of, or a substitute for expertise. … All sources are best thought of as opinions, some more authoritative than others, but all should be subject to careful reflection and comparison to what we know and believe.”

---

99
What are a particular terrorist group’s tactics and targets likely to be? These are the questions analysts can address but cannot answer definitively as they transform raw intelligence into finished intelligence and warning products. Almost always there is an underlying ambiguity, which can be seen as the fundamental difference between intelligence and information. With this in mind, we can now review the role warning plays in the state’s response to the challenge of terrorism.

**Aiding the Allocation of Resources**

Deciding where to allocate resources is a risk-based part of a counter-terrorism strategy. Countering terrorism is a resource-heavy undertaking in which no country has the ability to protect everything. Guided by warning assessments, security services can allocate their resources to protect individuals, groups, and locations (e.g. embassies, government buildings, and airports) which are at the highest risk. With sufficient time and threats of sufficient magnitude, warning might also be used to obtain funding for additional security resources.

The disruption of terrorist plans from warning can come about by deliberately alerting terrorists that their plans have been uncovered. Besides simply announcing publicly that a plot has been discovered, heavy-handed surveillance of known terrorists or their supporters is a more subtle option. Warning-led additional security measures, such as the installation of security barriers or changes in security operating procedures could delay the terrorists, or might even persuade them to abandon their entire operation. This would give police and intelligence services more time to neutralize the group. Consequently, when a predicted attack fails to take place, rather than an indication of a failure of warning, it may have been the result of successful, warning-induced countermeasures. This is hard to gauge, however, because it is often difficult to determine if the intelligence was accurate or whether the terrorists were engaging in a form of bluff to keep the authorities on edge. For these reasons, it is seldom possible to fully quantify the effectiveness of specific warnings in these circumstances to the public, security services, and especially to Congress.

Pre-emption of terrorists can occur through so-called premature arrest, that is one based on warning assessments before enough evidence for a successful prosecution has been acquired. Even if the terrorists are ultimately released, the arrest or detention itself often is enough to disrupt the plan and should be considered as a successful counter-terrorism operation. Given that the stakes in a successful terrorist attack are so great, it is no longer possible for law enforcement agencies to risk an attack by delaying action until the last minute in hope of acquiring further evidence. After 9/11, the FBI took this message on board and changed its priority from prosecution to pre-emption (see section on post-9/11 responses below).

Mitigation of terrorist attacks are made possible when governments are alerted to the possible nature of the attack. Armed with such knowledge, they can take additional security measures to enhance the detection of terrorists or to make it more difficult for terrorists to enter or approach potential targets. Installation or repair of security screening equipment, such as scanners at entrances, surveillance cameras, erection of security barriers, and closing of approach roads all could be put in place, given sufficient time. In addition to this, security personnel can be placed on high alert and their presence increased. A visible police presence might disrupt the terrorists’ plans, causing them to miscarry or to be abandoned. In this regard it is worth mentioning that US embassies overseas work closely with local security services to enhance their physical protection and warn US citizens and businesses to enhance their security posture.

Recovery from terrorist attacks, especially from a chemical, biological, radiological, or nuclear (CBRN) attack, would benefit enormously if governments have timely warning which identifies the likely means the terrorists will use. Armed with this information, specialized responders can be alerted, medical facilities, decontamination plans and equipment prepared,
and continuation of vital services and communications assured. The 2001 anthrax attacks in the US in the aftermath of 9/11 are instructive examples. Persons contaminated by some forms of anthrax do not die immediately, nor are most of them likely to die if treated with antibiotics. But, if they are brought to hospitals or allowed to leave the scene and present themselves to hospitals without being decontaminated first, they can, in some cases, spread the spores unknowingly in the ambulances, taxis, or private cars which brought them in. Not only does this risk spreading the anthrax over a far wider area, it also results in the shutdown of treatment by hospitals while they are decontaminated, thereby causing a cascade effect with major consequences for public health.

Warnings of this nature should also enable governments to identify experts on the type of the attack, particularly if it is CBRN, and have them available to give accurate assessments to the public. Failure to do so, risks leaving assessments to the media which inevitably will use advocates of the most alarmist interpretation. The author experienced this after the Oklahoma City bombing of the Alfred P. Murrah Federal Building in Oklahoma City on 19 April 1995. On the day of the attack, while teaching at Yale, I received a telephone call from CNN which wanted to know in my opinion which foreign terrorist organization or country could be responsible. When this author explained that, given the nature of the target, the location of the attack, and the fact that it occurred on the anniversary of the ending of the Waco siege in Texas, it was most likely an act of domestic terrorism, CNN immediately lost interest.

Public warnings present a special case. Besides possibly inducing terrorists to abandon their plan because it is no longer secret, the main purposes of public warnings are to increase public vigilance and motivation to take protective measures. Public involvement in reporting suspicious behavior or suspicious packages which have been left unattended can bring terrorists and their activities to the attention of the police as under the “see something, say something” initiative.

Avoiding crowded areas at potential target sites is another security precaution the public can be advised to adopt. An example of this behavior is to spend as little time in airport reception areas as possible by checking-in and proceeding through security as quickly as possible. Because these measures require behavioral modification, essentially the public must be induced into adopting them by alerting it to an existing threat. Consequently, with public warning there is a fine balance between releasing enough information to motivate but not enough to cause panic or unnecessary financial loss to businesses. A second problem with threat warnings as a motivator is that their impact lessens with time and is undermined by government reassurances that the situation is under control - reassurances which the government feels it must make in order to retain public confidence. Ironically, these reassurances can, in part, be the result of crisis management and response measures initiated by the warnings. This means that there is an inbuilt tension between the alerting and the reassurance aspects of warning.

Dissemination

Mechanisms for dissemination of warning messages are as varied as the agencies producing them. Generally, they can be grouped by their timeframe and specificity. As examples, I will use those which were in use by the Interagency Intelligence Committee on Terrorism (IICT) and its Community Counterterrorism Board (CCB) on behalf of the IC before and after 9/11. Assessments were equivalent to National Intelligence Council (NIC) memoranda. Their purpose was to provide long-range general analysis of underlying trends, terrorist groups, and to make complex subjects comprehensible, but not simple. When former CIA Deputy Director of Operations Jim Pavitt candidly admitted that while the CIA foresaw the threat Al-Qaeda represented but was unable to predict the exact type and location of its attacks, he spoke to the essence of the distinction between assessments and other forms of warning. Assessments are
essential to understanding the nature of terrorist groups and the threats they represent. Some terrorists have limited goals, use discrete and limited violence, and are amenable to negotiations: groups such as the IRA or the Basque nationalist ETA. On the other extreme, some have almost unlimited or apocalyptic goals; they seek mass casualties and are not willing to negotiate: groups such as Al-Qaeda or Aum Shinrikyo, later known as Aleph. Knowing the terrorists’ character is of great assistance to police, crisis managers, and crisis responders by allowing them to prepare for the type of operations they are most likely to face. Such assessments are not the sole prerogative of intelligence analysts; strategic warning is the area which is least dependent upon secret intelligence. For this reason, academic and other expert opinions, especially from private organizations (such as the Rand Corp., which for decades has assisted the US government), might be of greater value.

Advisories are much more focused on significant issues and limited in time-frame. An example would be travel advisories such as those issued by the Department of State for US citizens to avoid travel to Lebanon during the 1980s. This advice was usually based upon a rise in anti-US sentiments among some sectors of society, deterioration in the security situation, a political crisis, or intelligence that a terrorist group might be planning to target Westerners.

Alerts are warnings of specific, imminent threats. In the example above, alerts would be a proper response when intelligence indicated that the Lebanese militant group Hezbollah had specific plans to kidnap US citizens. Similarly, in 2011, Russian authorities were given a specific warning of an impending attack on Moscow’s Domodedovo Airport. The alert provided authorities with the exact location in the airport, the customs area at arrivals. At the time, Russian security forces were searching for three Chechen suspects. Russian intelligence services had an excellent idea which Chechen group was behind the planned attack and knew that this group sought to create mass casualties. What was not known was the timing. However, the airport authorities did not secure the area, transfer pick-ups away from the airport building, increase police surveillance, and issue a public warning. The result was that on 24 January 2011 a terrorist bomb killed 37 people and injured 183 more persons. This was a failure to act, not a warning failure.

Problems with Warning

There are certain inherent paradoxes in the nature of warning which impact on its ability to perform its mission.

Intelligence Agencies Own the “Alarm Bell” but not the “All-Clear Whistle”

Warnings are generally issued as the result of positive intelligence or analysis about a threat. But seldom is there positive intelligence or analysis that the threat has gone away – such as the neutralization of the terrorists through killing or capture. Consequently, analysts conclude that just because a threat did not materialize today it may materialize tomorrow or the day after. That leaves responsibility for staying on alert with the policymaker, who must consider the cost of an alert against the risk of prematurely ending it. An example of this lesson was the 7 July 2005 series of terrorist bombings in London, which killed 52 civilians and injured more than 700 others. The US National Security Agency (NSA) intercepted messages linked to Mohammad Sidique Khan, one of the principal members of the terrorist cell, revealing that he was in contact with Al-Qaeda trained militants in the US. This intelligence was passed to UK intelligence agencies. But US intelligence concluded at the time that nothing in his file indicated he was planning to do something in the UK.

During the summer prior to the attacks, the UK lowered its threat level, encouraging the Metropolitan Police to make officers available for the G-20 summit meeting in Gleneagles,
Scotland. Those officers were not available in London when the terrorists struck. It is unlikely that the additional officers would have made any difference, but the timing undermined public confidence.\textsuperscript{17}

\textit{Warning is a Consensus Position}

Warning is the product of bureaucracy, a process involving more persons than just the analyst are involved. Under the UK system, which is characterized by strong central control, intelligence agencies do not make intelligence assessments at all. Instead, they are produced centrally by Cabinet Office assessments staff which strives for consensus. In contrast, the system in the US is more adversarial, reflecting a weaker center. In my day, just after 9/11, although warning products (Assessments, Advisories, and Alerts) were issued under my authority, I first had to task one of the intelligence agencies constituting the IC to draft it, which, of course, involved the analyst’s supervisor approving the finished product, usually after peer review in that agency. Then I needed to submit it to the Warn 5 (Warning 5: CIA, DIA – Defense Intelligence Agency, NSA, FBI, and INR – the Department of State’s Bureau of Intelligence and Research) together with any other agencies with expertise, for their approval.

Dissent, should it occur, was recorded in “footnotes” reflecting differing conclusions. The salient advantage of both systems is their element of peer review, which reduces the element of bias on the part of the analyst. Such analytical problems are often the result of cognitive dissonance when analysts are overloaded with too much conflicting and inconclusive information. Under these conditions, analysts are predisposed to “cherry-pick” only those points that support their preconceptions while dismissing those in conflict with them. This is because one generally requires more information to revise prior conclusions than to confirm them.

There is also the risk of bias, on the part of the agencies themselves which can result in pressure on analysts when warnings or assessments conflict with policy initiatives. During the Iran/Contra Affair, the CIA attempted to use an assessment concerning the American hostages held in Lebanon by Hezbollah to justify the administration’s secret policy of selling arms to Iran, which was against the proclaimed policy of the Reagan administration not to make concessions to terrorists. In the end, the CIA’s efforts failed to sway DIA and INR analysts and the resulting Top Secret assessment concluded that “hostages were neither seized nor released without approval from Tehran.”\textsuperscript{18}

According to some commentators, the most nearly correct judgements in crisis situations often have been reached by a minority of individuals; when there are disagreements then, the inevitable question is whom to believe – the majority opinion or dissenting opinion of one agency or even one analyst.\textsuperscript{19} One of the most famous examples of this was the 2002 assessment that Iraq did have a nuclear program; INR dissented and the subsequent invasion and occupation of Iraq proved it right.\textsuperscript{20}

\textit{Warning is not a Commodity}

Warning is intangible, a hypothesis based upon probability. It is also a transaction between two parties; someone must give it and someone must receive, accept, and understand it. Policymakers often have other sources of information or can be skeptical of intelligence in general. After the Japanese attack on Pearl Harbor, one naval officer observed that, “Possibilities, capabilities and intentions become academic when one does not accept the credibility of his own estimates.”\textsuperscript{21} In other words, I’ll believe it when I see it, but I’ll only see it when I believe it. All too often, however, policymakers are disposed to reject warnings not because they are uncomfortable with uncertainty but because it conflicts with their pre-existing
views or is critical of their policy’s effectiveness. Michael Hayden, former director of NSA and CIA, observed President Trump doing this when he “rejected a fact-based intel assessment because it was inconsistent with a preexisting world view or because it was politically inconvenient …”22 The ideal was described by former Secretary of State, Colin Powell, when he told INR: “I hold you accountable for the facts, but not for your judgements even if later proven wrong.”23 Regardless of the intelligence, Colin Powell knew that the decision was his and his alone.

“The Drunk and the Lamppost”

An old joke in intelligence circles has it that just like the drunk leaning against a lamppost after a bender, policymakers want intelligence more for support than enlightenment. Few leaders, have had direct experience with intelligence agencies as George H.W. Bush as former head of the CIA and Vladimir Putin as former head of FSB had. For all too many of the remainder their familiarity and expectations often came from a Scottish actor introducing himself on screen as “Bond, James Bond.” Much as Bond movies are valued as entertainment, they leave policymakers with an inflated view of what intelligence can do for them. They often read intelligence briefs selectively, looking for confirmation of their beliefs rather than seeing a potentially valuable critique of them. Worse, they may press to see the raw intelligence which underlay the assessment, although they are untutored in evaluating it. It was for this reason that former Deputy Secretary of State Strobe Talbot instructed INR never to give raw intelligence to senior people.24 This is especially true for warning, because it imposes the need for a response on the policymaker, whether positive (acting) or negative (not acting). Warning’s key component is threat, which is the combination of the terrorists’ intentions and capabilities. In this regard, it is worth mentioning that threat and risk are not the same thing; risk assessment also includes consideration for society’s vulnerabilities and the countermeasures to protect these, while the role of warning is to help focus countermeasures on those areas most likely to be attacked.

This raises the question: what happens when policymakers feel they cannot afford to take adequate precautions because doing so would be too expensive or politically unacceptable? One option is to ignore the threat and by default accept responsibility for the heightened risk that results. Another is to pressure warning analysts to reduce their estimate of the threat. An example of the former was related to the author by Nicholas Pratt, director of the Program on Terrorist Strategic Studies at the George C. Marshall European Center for Strategic Studies, about an analysis done for the Bavarian police in preparation for the 1972 Munich Olympic Games, which foresaw an attack by Palestinian terrorists on Israeli athletes and was so prescient that it could have served as a commentary after the event. The scenario was one of 27 prepared by the contractor and it was ignored, possibly because the police found that it conflicted with showcasing the new Germany through a friendly and unarmed police presence.

Another example that is worth mentioning, is the suicide attack on the US Marine barracks on 23 October 1983 in Beirut. The attack was the consequence of the Reagan administration ignoring mounting evidence that the Marines’ presence in Lebanon as peacekeepers had been steadily undermined by US actions, such as the bombardment of Lebanese Hezbollah positions by US warships.25

In a reverse scenario, the 9/11 Commission, in faulting the failure of the IC to consider aircraft as a suicide weapon instead of as a vehicle for hostage taking, called for “institutionalizing imagination.”26 Wise after the fact, it selected from the spectrum of intelligence available only those items which indicated the former use, while ignoring the far stronger indicators for the latter. Unlimited imagination, however, is no substitute for analysis in the warning process, especially if the potential threat is unlimited such as when CBRN is involved. In November 2001, when Vice-President Cheney was briefed that Pakistan might be
assisting Al-Qaeda in making a nuclear weapon, he proclaimed that “if there’s a 1% chance that Pakistani scientists are helping Al-Qaeda build or develop a nuclear weapon, we have to treat it as a certainty, in terms of our response. … It’s not about our analysis or finding a preponderance of evidence. It’s about our response.” This reasoning undermines risk-based counterterrorism strategies, which free governments from having to concentrate their limited resources on such worst-case scenarios. It does this by converting hypothetical worst-case dangers into actual threats with enormous cost implications for foreign policy, national security as well as homeland security.

Intelligence can never be relied upon to get every threat scenario right but, if nearly all hypothetical threats were taken seriously, there would be no need for analysis. Ultimately, such a position would be self-defeating because the flood of warnings for unfounded hypothetical threats would soon obscure those for valid ones.

Even so, analysts must never consider the costs to government or society of issuing warnings as that would politicize analysis. The role of the analyst is to estimate threats; calculating the cost of countermeasures in response is the policymaker’s role. Likewise analysts must resist pressure from policymakers to inflate the threat level, either for political or budgetary gain. This separation of role is made much more difficult when the calculation of threat comes from analysts who work in the same organization as the policymakers who are responsible for implementing countermeasures against it.

**Structuring Intelligence and the Evolution of Warning**

Sherman Kent, who for 20 years directed the CIA’s Office of National Estimates, argued that intelligence is organization: “the staff, support, and controls needed to produce the actionable special intelligence that is vital to support the nation’s security.” Intelligence-derived warnings of terrorist operations or plans are an important part of that special intelligence.

Kent meant that good intelligence does not just happen, it is the product of processes inseparable from the bureaucracy that produces it. Intelligence, like some giant super tanker, cannot change direction immediately. Bureaucratic structures take time to evolve, analysts skilled for one field cannot immediately, if ever, reorient themselves for another, and hardware designed for one purpose cannot always or easily be redeployed against another. Reconnaissance satellites, for example, cost over a billion dollars and take decades to design and deploy. Since they are in essence in free-fall, they cannot be redirected significantly once in orbit.

**Organizational Development and Effectiveness prior to 9/11**

The official 9/11 Commission Report begins with a general indictment of the US government, including the IC:

“We learned that the institutions charged with protecting our borders, civil aviation, and national security did not understand how grave this threat could be, and did not adjust their policies, plans, and practices to deter or defeat it. We learned of fault lines within our government – between foreign and domestic intelligence, and between and within agencies. We learned of the pervasive problems of managing and sharing information across a large and unwieldy government that had been built in a different era to confront different dangers.”
Although there is much truth in this assessment, it fails to reflect the considerable efforts undertaken by the US government to adjust its structure and policies to newly emerging and ever-evolving terrorist threats. By tracing this evolution, it is possible to see that the success of the 9/11 attacks was, far from being a sweeping example of government stasis, an operational failure in a dynamic environment. Modern urban terrorism first appeared following the death of Che Guevara in 1967 with the rise of groups such as the Uruguayan Tupamaros, the Brazilian National Liberation Alliance, and the Argentine People’s Liberation Army. Other groups soon arose around the world: the Weather Underground in the US, in Japan the Japanese Red Army, in Germany the Red Army Faction, in Italy the Red Brigades, in the UK the Provisional Wing of the Irish Republican Army and the Protestant Ulster Defense Force, and in Spain the Basque Nation and Liberty (ETA). Israel’s victory in the 1967 Six-Day War led the Palestine Liberation Organization (PLO) to turn to terrorism and spawned a series of other Palestinian terrorist groups, often supported and at times directed by Syria, Libya, or Iraq.

The simultaneous hijacking of four civilian airliners in 1970 by the Popular Front for the Liberation of Palestine (PFLP) is regarded as the start of the modern era of terrorist “spectaculars.” Iran only began its rise to become the preeminent terrorist state-sponsor a decade later when in 1982 Iran helped to establish Hezbollah among Lebanon’s Shia population in the south of the country.

Initially, the US government could not see the forest for the trees. Guerrilla war was familiar, but with terrorism there appeared to be no discernible pattern as groups acted in response to their own agendas, capabilities, target vulnerabilities, and the existing political environment. Viewed by Washington as largely a police matter, counterterrorism policy was left to the Department of State’s geographic bureaus on the assumption that terrorism was nothing more than a manifestation of local problems. The CIA took a similar approach. Responding to a Department of State request for information about terrorists, the CIA noted: “the Agency deals with the problem of terrorism on a regional geographic basis by analysts trained in covering a wide range of activities in the countries they specialize on.”

One pattern soon emerged that could not be delegated: the escalation of violence, particularly amongst Middle-Eastern groups which were in loose cooperation and competition with each other. In order to retain media attention and to continue to instill fear in the public, terrorists began to make their attacks larger and more violent; hijacking of empty planes soon escalated into taking passengers hostage and then into the murder of one or more of them. Similarly, attacks, such as bombings, escalated into multiple simultaneous attacks. Likewise, suicide attacks initiated by the Popular Front for the Liberation of Palestine (PFLP) were soon copied by other groups as demonstrations of ultimate commitment by their members.

In response to the growing number and severity of incidents, particularly with the PLO’s Black September Organization’s attack at the Munich Olympics in 1972, President Nixon established a cabinet-level committee chaired by the Secretary of State to combat terrorism. This committee supervised an Interagency Working Group (IWG) consisting of over 30 agencies. At the end of the decade, the Department of State created an Office for Combating Terrorism to coordinate counterterrorism foreign policy.

On 15 September, 1972 CIA began publishing a “Weekly Situation Report on International Terrorism” (WSRIT). Distributed to senior policymakers, the WSRIT listed terrorist threats reported by intelligence and reviewed past terrorist operations for clues to future activities making it an early form of warning threat assessment. The first dedicated threat assessment unit, better known as the Threat Analysis Group (TAG) was created by the Department of State’s Office of Security (SY – the forerunner of the Bureau of Diplomatic Security or DS) in 1976. The TAG was “unique in that it had legitimate analytical and threat assessment responsibilities to monitor terrorism at home and abroad.”

President Carter transferred responsibility for counterterrorism from the Cabinet to the National Security Council and, following a 1977 review of US policy procedures, he
established the “lead agency” concept for managing terrorist incidents. Under this system agency roles were clearly delineated with responsibility for coordinating response to incidents abroad vested with the Department of State, response to domestic incidents with the Department of Justice (FBI), and response to incidents aboard aircraft with the Federal Aviation Administration (FAA). However, there still was no designation of responsibility for warning apart from the TAG’s role in the protection of US diplomats abroad and foreign dignitaries in the US. A 1982 IC assessment on the role intelligence played during the Carter administration noted that there was “continued focusing of policymaker attention on the crisis management and foreign policy aspects of the terrorism problem almost to the exclusion of consideration of the establishment and maintenance of a credible threat assessment capability.”37 This worked to the detriment of warning.

The pace of change quickened during the Reagan administration, which was largely concerned with state-sponsored terrorism. State-sponsors regarded terrorism as a policy tool used to send messages or to impose costs on other states for “unfriendly actions”. Seen from the Cold War perspective, proxy actions, as a form of statecraft, were for this reason more easily understood. One of the administration’s great concerns was Soviet assistance to the PLO, including the training, funding, and equipping of its fighters, as well as its Eastern Bloc’s provision of safehouses for them and of transit for terrorist teams. Poland and East Germany even allowed the Abul Nidal Organization (at one time considered to be the most dangerous terrorist group in the world) to operate businesses openly.38 But in dealing with Middle-Eastern state-sponsors, the administration lurched from military attacks (e.g. on Libya for the La Belle Disco bombing in Berlin which killed two American servicemen), to covert collaboration (e.g. during the “Iran/Contra affair” the US sold weapons to Iran in the hope of obtaining the release of US hostages and circumventing Congressional scrutiny of its illegal funding of the Nicaraguan Contras).39

In 1982, as a result of lessons learned from the kidnapping and rescue of US Brigadier General James Dozier in Italy, President Reagan established the Interagency Intelligence Committee on Terrorism (IICT) and served as its first chairman. In April that year, he issued a formal National Security Decision Directive (NSDD 30) to charter the IICT under the chairmanship of the Director of Central Intelligence (DCI).

The IICT was the primary forum for coordinating IC counterterrorism activities and for issuing warning products on behalf of the IC. Through its TIERS subcommittee, it produced the IC’s ranking of terrorist collection priorities which informed the allocation of resources. Its other functions were reflected in its permanent subcommittees: Warning, Nuclear, Biological, and Chemical Threat, Technical Threat and Countermeasures, and Analytic Training. Connectivity within the IC was an early and continuing responsibility through its management of an electronic community of interest - CT-Link. The IICT was the first recognition, in bureaucratic terms at least, of the importance of warning. The single greatest impetus for enhancement of US counterterrorism efforts during this decade came from the Vice-President’s Task Force on Terrorism. It led the President to reaffirm the role of the IICT with NSDD 207 in January 1986 and to transfer its direction to the National Intelligence Council (NIC) under the chairmanship of the Director of Central Intelligence (DCI).

Another recommendation of the Vice-President’s Task Force led to the establishment of the CIA’s Counterterrorist Center (CTC). This occurred in 1986 in order to centralize resources engaged in counterterrorism. The CTC was a fusion center which brought elements of CIA’s Directorate of Operations (DO) and Directorate of Intelligence (DI) together with representatives of the FBI, NSA, the Department of Defense (DoD), and other agencies (reaching a total of 30 by 2001). To further concentrate counterterrorism efforts and eliminate possible confusion of roles and responsibilities between CIA and the NIC, the NIO/CT was abolished and IICT transferred to the CTC, effective 1 November 1989. The CTC director then
created a Community Counterterrorism Board (CCB) under the Chairman of the IICT to act as its executive.

The CTC was directed to pre-empt, disrupt, and defeat terrorists.\textsuperscript{40} Although it reported to the Director of CIA, the majority of CTC managers came from the DO and looked to the Director of Operations for guidance.\textsuperscript{41} Since warning did not feature among CTC’s primary objectives, however, the IICT/CCB was tangential to the CTC’s perceived role. Consequently, an inspection of CTC in 1994 faulted its capacity to provide warning of terrorist attacks.\textsuperscript{42}

By these measures, the IC now had a centralized organization (CTC) to conduct the fight against terrorists overseas. Because the IC was not allowed to operate inside the US or to collect intelligence on US citizens, it was not responsible for combating or warning about domestic terrorism, a role that was reserved to the FBI and the Department of Justice. As 9/11 demonstrated, this was a point of weakness and potential disconnection.

In 1996, the CIA created the Bin Laden Issue Station (nicknamed Alex Station). Under the authority of the CTC, Alex Station was located in the Washington area and was the first virtual station and the first dedicated to a single issue. Its composition made it a miniature of CTC. Neither the CTC nor Alex Station were perfect; conflicts such as that between CIA, FBI, and DIA persisted.

Merging intelligence and law enforcement was still difficult because of their differing missions, legal authorities, capabilities, and bureaucratic cultures.\textsuperscript{43} For Intelligence, as noted, “truth” is unobtainable and assessment of probability is often based upon sources of uncertain reliability and deductions of analysts who never have all the information they need. Law enforcement is concerned with amassing evidence to demonstrate truth in a court of law. Intelligence for law enforcement constitutes “tips” and analysis, as performed by Intelligence Agencies, was until recently an alien concept.

The distinction between an Intelligence and Law Enforcement case can be illustrated by the suicide bomb attack on the USS Cole in Aden’s harbor in Yemen on 12 October 2000. In spite of the IC’s high degree of certainty, its judgement about the responsibility for the attack (which killed 17 US sailors and wounded 39 others) was described as “preliminary” so as not to lead law enforcement to commit to this finding before its own investigations were complete, which could have led to accusations that the administration was acting without conclusive proof.\textsuperscript{44} While they could do nothing about this fundamental difference in concepts of “proof,” centers, like the CTC, encouraged sharing of information by providing a secure, collegial environment and aided the development of mutual trust, for we begin by trusting individuals and only later by trusting their institutions.

In many ways the FBI recognized the rise of terrorism, but was unable to respond adequately to it. As far back as 1980, it had established its first Joint Terrorism Task Force (JTTF) with the New York Police Department. Located in the FBI’s New York Field Office, it was intended to assist New York Police cope with domestic terrorism. JTTFs expanded to other cities until there were 34 offices at the time of the 9/11 attacks. While these were the primary vehicles for investigating terrorist activity, most were, according to the 9/11 Commission, not fully staffed and state and local entities often believed they had little to gain from full-time participation.\textsuperscript{45}

Following the World Trade Center bombing of 26 February 1993, FBI Director Freeh told Congress that “merely solving this type of crime is not enough: it is equally important that the FBI thwart terrorism before such acts can be perpetrated.”\textsuperscript{46} To do this he created a Counterterrorism Division at FBI headquarters to replicate the CTC and arranged for the exchange of senior FBI and CIA officers. But changing the FBI’s traditional focus on organized crime, the key element in its preeminent Criminal Division from which came most of the FBI’s leadership, proved elusive. In 1998 the FBI issued a five-year strategic plan which for the first time made national and economic security, including terrorism, its top priority, giving prominence to the new Counterterrorism Division over the Criminal Division.\textsuperscript{47} But the FBI...
lacked the resources to fully implement this plan. One critical problem was the lack of properly trained analysts to process the information gathered by the FBI’s field agents. Another was the lack of trained personnel to put that information into a form that could be disseminated. This task was performed at the CIA by its reports officers and to assist the FBI resolve this bottleneck, CIA made some of its own officers available. Lastly the FBI’s filing system was a shambles resulting from neglect of its traditional paper files and the failure of a computer system that was supposed to have replaced them. As a result, the 9/11 Commission concluded that prior to 9/11 “the FBI never completed an assessment of the overall terrorist threat to the U.S. homeland.” Furthermore, the FBI persisted in withholding written reports about its pending investigations because Federal Law prohibited such disclosure in cases which might go before a Grand Jury.49

FBI effectiveness was further undermined by the misapplication of procedures initially intended to regulate sharing of information between the FBI and Department of Justice prosecutors. The situation grew more confused as restrictions on sharing information authorized as intelligence collection by FISA Courts (Foreign Intelligence Surveillance Act) were interpreted as prohibiting sharing with FBI agents working on criminal investigations. This created what became known as “the Wall.” Ultimately, the FBI came to believe that no intelligence could ever be shared with the Criminal Division even when no FISA Court authorization was involved. This also prevented intelligence gathered by the CIA and NSA from reaching criminal investigators.50

**Overseas Initiatives**

US interests, citizens, and facilities abroad had always been favored targets for terrorists; by 1980 approximately one-third of all terrorist attacks were aimed directly at US personnel or institutions around the world. In response, the Department of State undertook a multimillion-dollar security enhancement program to improve physical security at its US embassies and consulates and established the Bureau of Diplomatic Security to oversee security measures in US foreign missions and protect foreign diplomats at the UN.

Success in reducing terrorist attacks against diplomatic targets came at a price; as “official America” became more difficult to attack, terrorists compensated by turning their attention to “corporate America.”51 In order to discharge both its moral and legal responsibility towards Americans overseas, the Department of State created the Overseas Security Advisory Council (OSAC) to coordinate security and instituted Travel Advisories to provide guidance and warnings to the general public.52

On 21 December 1988, PAN AM flight 103 was blown up by a terrorist bomb over Lockerbie, Scotland, killing all 270 on board, including 189 Americans. An investigation by the President’s Commission on Aviation Security and Terrorism found that on 5 December 1988 the US embassy in Helsinki had received a threat that within two weeks a bomb would be placed on a PAN AM flight from Frankfurt to the US. The Commission further determined that this threat had been distributed selectively by the FAA and the Department of State, leading to the accusation of a double standard by warning government employees and not the general public.53 In 1990, the Congress required, as part of the Aviation Security Improvement Act (Section 109), that the President “develop guidelines for ensuring notification to the public of threats to civil aviation in appropriate cases” - known informally as the “no double standard” policy. In response, the FAA began providing airlines with Aviation Security Bulletins and the Department of State expanded the notification requirement to include non-aviation threats.54

Watchlisting terrorists is not always considered a warning function, but it actually plays a key role in warning. Just the knowledge of an attempt to enter the US can be a valuable warning indicator of an impending operation as well as a potential means of frustrating it.
The Department of State’s watchlisting program (TIPOFF) was unique because it was the first successful attempt to overcome the barrier between the closed community of secret information and the open world beyond it. Remarkably it was the product of a single INR analyst, who almost unaided conceived, executed, and initially ran the system. TIPOFF, like every watchlisting program, was actually a system involving three key functions: all source data collection, processing and storage in a secure environment combined with a robust capability for finding individuals quickly and accurately, and sharing identifying information on the terrorists beyond the secret world of the IC. TIPOFF’s purpose was to aid consular officers overseas and immigration officers at US ports-of-entry (POE) identify suspected terrorists attempting to enter the US. “Hits” were referred to TIPOFF which then coordinated with the IC.

TIPOFF was able to watchlist suspected terrorists on the basis of “reasonable suspicion,” such as association with known terrorists. Many of the 9/11 participants, for example, had no previous “terrorist record” but some were known to associate with Al-Qaeda operatives. Since foreigners had no inalienable right to enter the US, this was enough to deny a visa or refuse entry. TIPOFF also negotiated agreements with Canada and Australia governing the sharing of lookout information and control of secret information, demonstrating the possibility for creating a global lookout system for terrorists.

By 9/11, TIPOFF was the best terrorist watchlist in the US government, but it was not perfect. Reflecting its origins as a border-security support system, it was never intended to be a comprehensive listing of all known terrorists; it was not authorized to hold information on, or to watchlist, US citizens (and alien residents) because they had a right to enter the US and, in any case, the IC was not authorized to collect or store information on US citizens. Its other weakness reflected its origins. As the work of a single analyst and not an IC initiative, the IC did not fully recognize TIPOFF’s importance or sufficiently commit to supporting it. In spite of a Presidential Decision Directive (PDD 62) directing CIA to ensure that names of terrorists were to be disseminated to the Department of State, INS (Immigration and Naturalization Service), and FBI so that the border agencies could place them on watchlists, CIA only urged its personnel to support TIPOFF by submitting data on foreign terrorists and left responsibility with the individual without oversight. As the old adage goes “when everyone is responsible, no one is responsible.” This was to have dire repercussions on 9/11.

**Counterterrorism and Warning Efforts Prior to 9/11**

With the passage of time perhaps we can make a more balanced appraisal of the IC’s efforts to meet the emerging threat of international terrorism.

The most obvious question that was asked by the 9/11 Committee: “what was the overall strategy to counter the terrorist threat to the United States from 1985 to the present?” CIA’s response was: first, to take the offensive to disrupt terrorist networks and terrorist activity; second, integration of operational, technical and analytical elements in a single large unit collocating analytical and operational activity; and third, community orchestration by serving as the focal point for IC support on terrorism.

For all its shortcomings, missteps, and ultimate failure to thwart the attacks on the World Trade Center in 1993 and 2001, the US had developed new, and transformed existing, counterterrorism structures to implement its strategy. The definitive form of US counterterrorism efforts prior to 9/11 was determined by President Clinton in 1998 under PDD 62 and 63. Together these presidential decision directives defined the nation’s critical infrastructure, considered ways of protecting it, and confirmed responsibility for domestic counterterrorism with the Department of Justice and the FBI and with the Department of State and the CIA for foreign terrorism. It is true that these changes were made retrospectively, usually in response to significant terrorist incidents, such as the kidnapping of General Dozier
in Italy and attacks on US facilities abroad. This leads critics to argue that the US was preparing to “fight the last war over again”; but this was inevitable.

Major transformative change, such as the creation of the Department of Homeland Security, was never undertaken on hypothetical justifications, consequently what changes were made were largely internal within the IC and Law Enforcement agencies – creation of the IICT, the Department of States’ Office for Combatting Terrorism and Bureau of Diplomatic Security, FBI’s Counterterrorism Division, and especially CIA’s Counterterrorist Center and Alex Station. Such structural changes are relatively easy to make in comparison to changes in bureaucratic culture. Interagency centers, as noted, were important steps in overcoming long standing rivalries and building mutual cooperation but even so it takes time to change attitudes, more than was available before 9/11.

One key flaw was the lack of sufficient terrorism analysts. After three decades of fighting terrorism, there were only approximately 200 analysts throughout the IC specializing in terrorism, most of them at the CIA. According to its public statement: “prior to September 11 (2001), CIA had about 115 analysts including those assigned to CTC itself, who were working terrorism related issues or applying specialized skills to the overall terrorism problem.” Their primary purpose was to support covert operations against terrorist organizations and individual terrorists. With regard to warnings, however, the DCI noted that a 2001 inspection of CTC gave its CCB high marks for being an “honest broker” in facilitating and deconflicting views of the community on threat warnings.

James Pavitt, CIA’s Deputy Director of Operations, explained the shortcoming that led to 9/11:

“We’ve had a number of significant successes over the years, but the fact remains, and I think it’s important that I cite this, that we in the Government of the United States as a whole could not … prevent or precisely predict the devastating tragedy of the September 11 attacks. Why do I say that? The nature of the target - we had very good intelligence of the general structure and strategies of the Al-Qaeda terrorist organization, knew and we warned that Al-Qaeda was planning a major strike … what didn’t we know? We never found the tactical intelligence, we never uncovered the specifics that could have stopped those tragic strikes…”

CIA Director Tenet was certainly aware of the threat posed by Osama bin Laden. He testified in an open hearing before the Senate Select Committee on Intelligence (SSCI) in February 2000: “Everything we have learned recently confirms our conviction that (Bin Laden) wants to strike further blows against America,” and in February 2001, again before the SSCI, he warned “Bin Laden is capable of planning multiple attacks with little or no warning.” Not only was the CIA aware of bin Laden’s general intentions, CIA’s President’s Daily Brief of 4 December 1998, noted, “reporting – suggests Bin Laden and his allies are preparing for attacks in the US, including an aircraft hijacking to obtain the release of Shaykh Umar Abd al-Rahman, Ramzi Yousef, and Muhammad Sadiq Awda … the same source said … that two members of the operational team had evaded security checks during a recent trial run at an unidentified New York airport. …” This certainly qualified as an advisory, if not an alert. Despite its operational failures (see below), it can be argued that the IC got the overall threat assessment of Bin Laden right and warned of one of his likely tactics. Ten years after 9/11, Dan Byman, a professional member of the 9/11 Commission, reflected that: “the intelligence community repeatedly and consistently provided strategic warning that Al-Qaeda was going to attack. George Tenet testified on this publicly before 9/11, and the record is clear of his trying to warn policymakers in both administrations.” By concentrating on Al-Qaeda, the DCI actually took a “minority” position. Academics and the media at the time were more concerned with the
terrorist threat posed by Iran, its surrogate Hezbollah, and the IRA. They probably had valid reasons for this, as in the recent past Iran and Hezbollah had been more effective in killing Americans.66

In the end it was irrelevant whether Bin Laden intended to hijack planes to exchange their passengers for prisoners in US prisons or to fly them into buildings, the salient points were that such a plan was underway and its operatives appeared able to enter the US. And there was “objective evidence” supporting this assessment. On 19 November 1999, Hamidan al-Shalawi attempted to force his way into the cockpit of America West flight 90. Al-Shalawi and a second Saudi were taken into FBI custody but never charged.67 He was entered into TIPOFF and when he reapplied to enter the US on 5 August 2001 in Riyadh, his visa was denied. The FBI now believes al-Shalawi’s actions had been a dry run for 9/11.

Combined with CIA warning briefings, this incident could have persuaded the government and airlines to reinforce cockpit doors, place additional air marshals on flights, and enhance airport screening, but it was not declassified until years after 9/11. It was a warning that could, but did not happen. Other, vaguer, warnings were given, however. On 2 July 2001, the FBI’s Counterterrorism Division sent a summary of terrorist threats from bin Ladin to federal agencies as well as to state and local law enforcement agencies. This summary did not refer to specific types of attack or recommend specific countermeasures.68 Possibly in consequence of this failure, the US took no comprehensive steps towards improving airport screening and security on flights.

As for the CIA, its best remaining option was to alert the FBI directly and watchlist known Al-Qaeda members. Unaccountably, the CIA failed to do either, allowing two future hijackers, Nawaf al Hazmi and Khalid al Mihdhar, to enter the US undetected, although CIA knew their nationality, passport numbers, and that they both had been in the US and still possessed US visas. Had the CIA done so, it is quite possible both terrorists would have had their visas cancelled or been arrested on or after entry, possibly causing the plan to abort.69

Rather than a failure of the IC’s organization or of its underestimating the threat posed by Bin Laden or failing to warn about that threat, 9/11 ultimately was an operational failure accountable in part by the nature of the 9/11 plot itself. For while CIA was responsible for foreign terrorists and FBI for domestic terrorists this plot involved foreign terrorists attacking inside the US - a scenario which unintentionally exploited their division of responsibility.70 But it also reflected a failure to recognize the importance of watchlisting. When these terrorists sought to return to the US, it was a warning indicator that Al-Qaeda’s plan was underway and an opportunity to stop it. Finally, it reflected the abiding reluctance of IC members to share information.71

Post 9/11 - Bin Laden and Beyond

The attacks of 9/11 were so momentous that they resulted in a paradigm shift both in appreciation of the risk terrorists posed for society and in the size and scale of the response. In light of the damage wrought by bin Laden, this new form of terrorism was known as “catastrophic terrorism.” It is characterized by rigid religious views impervious to challenge on moral grounds, greater willingness to die, and greater lethality, with few inhibitions on targeting civilians or using CBRN.72

Confronting this post-9/11 reality a much-chastened government and especially IC began to transform themselves. US priorities were defined as: defend the homeland, defeat global terrorist networks, diminish the capacity of new groups to form, and deny terrorists safe havens. Yet these new priorities were in many ways just modifications of existing goals. The real difference lay in the realization of what would be required to achieve them. What was new was the underlying understanding that fighting the new terrorism would have to be a community effort, requiring fusion of intelligence, law enforcement, military and diplomatic responses,
together with new partners at the federal, state and local level who were responsible for homeland security, border security, crisis management and crisis response. That entailed fixing responsibility among new and old players, with recognition of the primacy of warning and risk-vulnerability calculations. Successful implementation needed the creation of permanent structures to institutionalize and communicate warning not just within government, be it federal, state, or local, but throughout the entire population.

The first step towards reorientation came in September 2001 with the restructuring of the National Security Council as terrorism was split from infrastructure security. This was followed by the creation of a parallel organization: the Homeland Security Council, first headed by Governor Tom Ridge, who went on to become the first Secretary of the Department of Homeland Security (DHS), when that department was established.

The new department brought together agencies responsible for domestic security: Coast Guard, Transportation Security Administration (TAS), Federal Emergency Management Agency (FEMA), Immigration and Naturalization Service (INS), US Customs, Border Patrol, and Secret Service (which soon may revert to Treasury). Full integration into the IC was critical to the fulfilment of several of its missions, notably to perform vulnerability studies and map threats against vulnerabilities; set national priorities for infrastructure protection; and, most importantly, to issue warnings directly to the American people. Accordingly, it set up a new intelligence unit under an Assistant Secretary for Analysis, which became part of the IC as well as the Warn 5 group (creating the Warn 6), which reviewed all IC warning products. In addition, DHS’ Homeland Security Operations Center (HSOC) was made responsible for warning federal, state, and local officials as well as the private sector and the public through its National Terrorism Advisory System (See Public Warning below).

In parallel with the FBI’s JTTFs, HSOC is connected to Antiterrorism Task Forces (ATTF), which now can be found in every state and most major cities throughout the US, and with private sector security programs through the American Society for Industrial Security (ASIS). ASIS members received a daily unclassified report from DHS and reported back any suspicious activity.

Warn, and through it, protect America became the watchword. The IC itself was transformed in recognition of the importance of warning. At its apex was a new Director of National Intelligence (DNI). The DNI is supposed to be a central hub for coordinating the IC – a role the DCI, it was thought, could not play because of rivalries between agencies, particularly FBI and DIA with CIA - and would be able to oversee domestic as well as foreign intelligence collection, something the DCI could not do. At the time it was believed that the head of the IC should not be both one of the advocates and the judge of them all in setting priorities for funding. There are issues, however, particularly with the enhanced risk of politicization as US presidents are not required to appoint individuals with an intelligence background. Such an issue emerged when the new DNI, John Ratcliffe, a Trump loyalist, notified Congress that there would be no further in-person intelligence briefings on foreign interference in the 2020 elections. In their place classified memoranda would be provided, but the change gave rise to accusations that it was intended to stifle Congress’ ability to question the DNI about Russian interference.

Reporting directly to the DNI are the NIC and a newly created organization, the National Counterterrorism Center (NCTC), which began operations in December 2004, subsuming the Terrorist Threat Integration Center (TTIC). TTIC itself had been created in June 2003 to close the seam between analysis of foreign and domestic terrorism. Drawing staff from throughout the IC but principally from the CTC, its key function was threat analysis and warning. TTIC took over CTC’s responsibilities for maintaining a threat matrix of all known terrorist plots against the US.

Twice daily TTIC conferred with FBI and other agencies via a secure video teleconference at which the matrix was reviewed and actions agreed upon. It drafted Senior Executive
Intelligence Bulletins and Executive Memorandums as well as spot commentaries. TTIC also assimilated the ICT with its warning functions and responsibility for connectivity. After 9/11, CT-Link, which became TTIC On-Line, grew to over 100 member agencies and departments, including representatives of all three branches of government, making it the largest classified community of interest in the US government.

When it solved the problem of warning with new organizations, the IC inadvertently contributed to another: the chronic shortage of trained terrorism analysts. As noted, on 9/11 there were hardly 200 available within the entire Federal Government. Now that warning in the form of TTIC was separated from counterterrorist activities in the CTC, those analysts who had transferred from CTC to TTIC were no longer available to support its operations and vice versa. Creation of the NCTC and intelligence centers and cells in agencies, such as DHS, throughout government further contributed to the already critical shortage of analysts, who were needed more than ever as more intelligence on terrorism began to flood in.

According to its director, the NCTC was the result of the 9/11 Commission’s recommendation for a “civilian-led unified joint command for counterterrorism.” Pursuant to this role, the NCTC prepared a National Implementation Plan for Counterterrorism (NIP) containing four pillars: (1) protect and defend against terrorists, (2) attack their capacities to operate, (3) work to undermine the spread of violent extremism, and (4) prevent terrorists from utilizing WMD. Established in June 2007, the NCTC’s Interagency Task Force (ITF) is charged with ensuring US government counterterrorism activities are “correlated rapidly” in response to changes in the “threat picture and level of risk” and formulates domestic and overseas options for senior policymakers.

Interestingly, for an agency created from TTIC, nowhere in the director’s summary of its priorities and role did the word “warning” appear. The NCTC does develop and facilitate national, international, and local exercises and shares lessons learned with DHS and FBI—contributing to the pre-emption and mitigation roles of warning, but domestic (public) warning is now vested with DHS. One consequence of this realignment was to place responsibility for domestic warning of terrorist threats and their mitigation and response in one agency, which could lead to conflicts of interest as indicated above.

TIPOFF was a victim of its own success. There was no other program for declassifying and using intelligence to identify terrorists, nor was there another comprehensive database for all-source terrorist intelligence. But the terrorist attacks of 9/11 demonstrated that the threat was ubiquitous and certainly could include US citizens. TIPOFF was transferred to TTIC and now has two successors. The first is the Terrorist Identities Datamart Environment (TIDE) which is a compendium with over 25,000 US citizens among its one million plus entries. The second is the FBI’s Terrorist Screening Center’s Database and its No-Fly List.

During that period, the FBI transformed itself, making terrorism and warning key priorities. This change was reflected structurally by combining its Counterterrorism, Counterintelligence, and Intelligence Divisions into a National Security Branch, officially on 12 September 2002, and by performing triage on its organized crime activities by transferring 900 special agents from crime to terrorism (and hiring hundreds of others) – leaving many of its traditional criminal investigations to be conducted by other law enforcement agencies. Another priority was Domain Management – a program to move beyond chasing criminals to gathering intelligence. An ex-CIA analyst was responsible for the program which has had problems similar to the Wall – fear of uncontrolled domestic spying. This was in spite of passage by Congress of the ‘Patriot Act’ in 2001, which introduced sweeping changes in how electronic surveillance was to be conducted and how financial transactions were to be accessed, among other areas. The Act’s intention was to improve sharing of information among law enforcement agencies, regulators, and financial institutions.

The FBI took a leadership role in liaison with state and local police officials. It established secure (classified) connectivity by constructing Sensitive Compartmented Information
Facilities (SCIF) within its regional offices’ JTTFs. Governors and key officials, as well as state and local police, now were able to access secure intelligence through TTIC On-Line in these SCIFs. Cooperation was a two-way street as locally obtained information could now flow back to Washington, making local authorities both producers as well as consumers of intelligence.

**Instituting Effective Public Warning**

This arrangement had its drawbacks, however. It was not inclusive enough. Essentially key officials were admitted into the “secret club” but this was not the same thing as public warning. To make public warning effective the IC had to transform its intelligence into information that could be widely/universally disseminated to private citizens. Credit for first undertaking this transformation goes to NSA which began including unclassified attachments on its TOP SECRET intelligence products. The IICT/CCB broke new ground when it published the first joint FBI/CIA terrorist threat assessment in both a secret and unclassified format. It also organized an open conference on suicide bombers, which resulted in guidelines for security officers on key behaviors and suggested countermeasures.

There were still problems with this solution. It is far easier to share general analysis or conclusions, which by their general nature make it easier to protect sources and methods, than it is to share highly sensitive intelligence about terrorists’ specific intentions. Unfortunately, this is in inverse proportion to the utility of the information for homeland security officials. They need to know which specific targets are most at risk so that they can best allocate their always limited resources in an environment containing almost unlimited vulnerabilities.

Public warnings through color-coded warning systems were not the answer. In May 2011, the US gave up its much-maligned color-coded Homeland Security Threat Advisory System. New York and Arizona already had abandoned it and few mourned its passing. Its major flaw was that it was constantly “on.” Blue and Green signifying all’s quiet were never used because they did not reflect world terrorist levels; red was impossible to sustain because of its effect on the economy; and consequently, it fluctuated between yellow and orange. In the words of Congressman Bennie Thompson: “The old color-coded system taught Americans to be scared, not prepared. Each and every time the threat level was raised, very rarely did the public know the reason, how to proceed, or for how long to be on alert.”

A warning system that is constantly blinking danger ultimately desensitizes people to the reality of the threat when it actually occurs.

It was replaced by DHS’ National Terrorism Advisory System (NTAS), which only has two elements: Bulletins (old assessments), which communicate general developments or general trends and Alerts, which communicate information about credible threats. There are two types of Alert: Elevated (old advisories) when there is only general information about the timing and target and Imminent (old alerts) if there is information that the threat is credible, specific, and impending. Alerts contain a “sunset provision” that marks their expected expiration date. The new system is designed to provide clear, timely, and above all specific information about the threat.

The reverse is also a problem with warning when there is too much, rather than too little intelligence. In such a situation analysts or customers drown in terabits of useless data. We do not have enough analysts to wade through all the material being collected by our own intelligence and law enforcement agencies as well as that passed to us from foreign ones, and obtained from world-wide open sources. In managing this shift from “cleared to know” to “need to know,” one must be mindful that intelligence sharing must not be sharing everything to everybody. Just as DHS has done with its NTAS, intelligence information must be disseminated according to need: on the grand scale to give the big picture with information about groups, their supporters, funding, recruitment, training, objectives, and capabilities; as
well as, on the individual scale, the activities, movements, and connections of individual terrorists. One last point, the interface of intelligence information and regulatory agencies who are responsible for watchlisting and blacklisting individuals or organizations, involves the implicit obligation to establish procedures to vet and review information and to remove the incorrectly or falsely accused quickly.

Conclusion

“Deye mon, gen mon” (beyond the mountains, more mountains) is an old Haitian proverb meaning beyond today’s problems lie still more problems. This is an apt metaphor for our ongoing involvement with terrorism for, in the words of Australian criminologist Grant Wardlaw, “there is no cure for terrorism, not through massive security measures at home and the projection of military force abroad.”90 This is not a counsel of despair, for just as we cannot eliminate terrorism any more than we can ordinary crime, we still can minimize it, reduce its impact, and anticipate its changing forms.

Between 2001 and 2018, the US spent at least $2.8 trillion USD on counter-terrorism, which according to the Stimson Center, is approximately 15 per cent of the US government’s discretionary budget. Most was spent in Iraq and Afghanistan, but $979 billion USD went to homeland security, representing about 35 percent of the counterterrorism budget. For that sum the US eliminated Bin Laden, diminished Al-Qaeda, and assisted in the dismemberment of ISIS. In view of this, it is noteworthy that during this period, only 100 people were killed on US soil as a result of Islamic terrorism.91

Although some terrorist threats have been diminished, we should never forget that terrorism’s enduring threat lies not only in the damage it inflicts but also in the psychological impact it has, namely by promoting panic and overreaction.92 While traditional groups, remain a threat, terrorism’s new frontiers lie, for the moment at least, with independent cells or lone-actors, who in addition to the traditional bomb, bullet, hijacking, and kidnapping may turn to novel forms of attack such as sowing computer viruses or ransom ware, hacking systems, or employing CBRN agents. These actors may be joined by “professional” protestors who target international meetings, such as the G-20, and exploit demonstrations against local grievances in the hope of provoking government over-reaction. Conceivably they could return to the domestic terrorism which plagued the 1970s. And they may be joined by others such as right-wing, Neo-Nazi, and neo-anarchist groups and individuals.

Warning in the form of identifying and calculating the risks posed by these actors and their methods will require looking beyond the threats themselves at their secondary effects – especially to the environment. It will need to be focused on assisting state and local authorities, especially police and first responders identify these novel threats and guide them on how best to respond to them, as the NCTC is now doing. One thing is certain, the IC and US government must recognize that failure to warn prior to a terrorist attack results not just in physical damage to society but also in diminished confidence in those agencies responsible for protecting citizens, especially when it is later revealed that information was withheld that could have prevented loss of lives. This cost of loss of public confidence generally outweighs the costs of divulging secret intelligence.93

As a UN Report notes: increased scrutiny for potential male suicide bombers who may be disguised as females may make transgender
persons, transvestites, and intersex (those in the midst of a sex change process) susceptible to increased harassment and suspicion. This admittedly is an extreme case but inevitably there will be trade-offs between respect for the rights of individuals and organizations (such as mosques) and the protection of society. Where to draw the line is of fundamental importance if we do not wish to sacrifice our way of life in order to protect it.

Throughout this chapter, this author has been guided by Sherman Kent’s observation that intelligence is a matter of organization; you get the intelligence and warning you prepare for. This raises similar questions to those asked about the IC prior to 9/11: whether after spending billions on a revamped IC just how fit for purpose is it today in dealing with mini-cells and individual terrorists and whether it is the proper agent to do so?

Terrorists are often funded through petty crime, recruited in prisons, and exhibit behavioral changes noted by their local communities and so domestic collection today is best undertaken by local law enforcement and the FBI. The IC can best contribute to protecting society by continuing to fight foreign terrorists, first by enhancing the sharing of intelligence through a network of sister fusion centers around the world, second, by continuing to turn intelligence into information that can be shared widely outside as well as inside the US, and finally, by supporting and encouraging watchlisting with foreign partners, as was initiated by TIPOFF with Canada and Australia.

As we plan tomorrow’s Intelligence Community, we should not do so on the basis of either the present terrorist threat or the past one, represented by 9/11. Today’s new terrorism is not the sole or main threat to domestic or global security and the IC’s efforts at collection, analysis, and warning will need reflect this. State-sponsors such as Iran and its primary surrogates, Hezbollah and Iraqi Shia militias, remain active. A new state-sponsor and worse has reemerged with Russia’s activities in Ukraine. Failed or failing states, such as Somalia, Libya, Afghanistan, Syria, Venezuela, and Yemen may spawn potential terrorist threats.

While terrorism is important, so too are more traditional global threats: emerging nuclear powers North Korea and Iran, conflicts between nuclear powers such as India and Pakistan, and the rapidly emerging super-power China, to name a few. The relatively new threats of computer hacking and denial of service attacks are escalating dramatically. In 2007, cyber hackers targeted Estonia’s parliament, banks, government, and media, giving a foretaste of what future cyber-assaults could do as dependence on cyberspace continues to grow. Russia’s attempts to manipulate the US presidential elections in 2016 and 2020, the UK’s Brexit and Scottish independence votes, as well as other elections in Europe, reflect the dawn of a new electronic Cold War. Russia, China, and Iran, in particular, are developing robust capabilities in this field. This will be a challenge for the IC and warning because it unites threats from states, international criminal organizations, cyber-terrorists, and individuals and will require new partners and new skills to identify new threats as they evolve and to provide timely guidance in defeating them.

Finally, in recognition of the enduring threat of terrorism, we have seen new agencies emerge, particularly to warn and protect the homeland. Such institutionalization of our counterterrorism efforts serves to fix responsibilities but also massively increases the size of the bureaucratic pyramid. We must be mindful of the over-specialization this can entail. Specialization does not always lead to greater effectiveness; it can also lead to the endless production of reports, bureaucratic empire building, and maintenance of hierarchy. The impact of these tendencies can be debilitating because intelligence analysis and warning depend upon initiative, integrity, and freedom from politicization that are difficult to accommodate in ever growing bureaucracies. A decade ago, Harold Ford, one of CIA’s premier analysts, cautioned: “In the last analysis, however, improvements will not rest so much on organizational or procedural changes, whatever their nature, as on the caliber, cooperativeness, and integrity of the individual officers who produce intelligence. And even more on the caliber, cooperativeness, and integrity of the individual officers who consume intelligence.”
Kenneth A. Duncan is a retired US Senior Foreign Service Officer. On September 5, 2001, he became Chairman of the Interagency Intelligence Committee on Terrorism and its Community Counterterrorism Board. In this capacity he was responsible for providing formal warning of terrorist threats on behalf of the Intelligence Community to the highest levels of the Federal Government and for formulating and levying intelligence collection requirements on the Intelligence Community. Prior to his selection for this post by the Director of Central Intelligence, he was Charge d’Affairs, a.i. at the US Embassy in Haiti. He also served in the Department of State’s Bureau of Intelligence and Research (INR) as Director of the Office of Intelligence Coordination and as Deputy Department representative on the National Counterintelligence Policy Board. As such he was Senior Advisor to the Secretary of State for all matters involving counterintelligence and sensitive law enforcement activities. He also served as the analyst for Middle-Eastern terrorism in INR and taught courses on terrorism at Yale University and at the United States Coast Guard Academy. On retirement from the Foreign Service, he became Senior Adjunct Professor of Terrorism at the George C. Marshall European Center for Strategic Studies in Garmisch-Partenkirchen, Germany.
Endnotes


3 ‘Yemen parcel bomb was 17 minutes from exploding’, BBC, 4 November 2010. The two bombs were discovered after a Saudi tip-off.


7 Related by former KGB Major General Oleg Kalugin in conversation with the author.

8 MI5 provides a publicly accessible website on terrorist threats. Available at: mi5.gov.uk and gov.uk>terrorism-national-emergency. The State of Connecticut uses a reverse 911 calling system in order to disseminate emergency information to the general public. Available at: ct.gov/CTAlert.

9 Peterson 2011, p. 4


12 These Assessments, Advisories, and Alerts were drafted by member agencies of the IC, approved by it, and issued in its name. See the following section for details.

13 DCI Counterterrorist Center booklet, June 2002.


17 Ibid.


Hayden, Michael, Gen. Michael Hayden on Perils to Intelligence in the Cyber Age. Real Clear Politics, 21 May 2018; Available at: realclearpolitics/video/2018/05/21/full_video_gen_michael_hayden_on_perils_to_intelligence_in_the_cyber_age.

Instructions to INR’s Director.

One reason for this caution was that many times ‘intelligence’ was manufactured by industrious informants because the US was paying for it. In Lebanon it was a cottage industry and so prolific that it gave rise to the term ‘rumint’ referring to rumor passing for intelligence.

Martin and Walcott 1988, pp. 125-160. The Marines on duty were carrying unloaded weapons and had orders only to fire if fired upon.


I am indebted to the former CTC’s Deputy Director for Analysis for these insights. They were in conversation with the former Deputy Director of the IJCT/CCB on 28 February 2002.

As occurred during the Reagan administration, when it sought to revise statistics on international terrorist incidents to include threats. The effect of this change would have been to double the annual number of incidents. The possible motivation for this change was to justify a tougher foreign policy. See: Pluchinsky 2020, p. lxxxii.

Kent, Sherman, Intelligence for America’s World Policy, Princeton: Princeton Legacy Library, 2015. For the role Sherman Kent played in the development of CIA’s analytic capabilities, see Davis, Jack, ‘Sherman Kent and the Profession of Intelligence Analysts,’ The Sherman Kent Center for Intelligence Analysis Occasional Papers, Volume 1, No 5, 2002.


Pluchinsky 2020, p. 309.

Duncan 1997, p. 187. Reflecting its growing importance, in 1979 its director, Anthony Quainton, was appointed to the rank of Ambassador while representing the US in international fora. L. Paul (Jerry) Bremer was made the first Ambassador-at-Large for Counterterrorism in 1987 in order to raise further the office’s profile, but it was only in 2012 that the Office was elevated to Bureau status.

Pluchinsky 2020, p. 167.

Ibid., p. 314.

Ibid., p. 416.

Duncan, p. 188.


DCI Counterterrorism Center Booklet, p. 7. Reflecting its role to go after terrorists, the CTC was named the Counterterrorist Center rather than the Counterterrorism Center.


Ibid., p. 92.

Wright, Lawrence, The Looming Tower, London: Penguin Random House, 2011, p.274 ff. Alex Coleman, the first FBI agent assigned to Alex Station, was first viewed as a spy by Station Director Michael F. Scheuer. Coleman’s mission was to gather evidence with the goal of prosecuting Bin Laden, but the only person truly interested was John O’Neil in the FBI’s New York Field Office. (New York had responsibility for bin Ladin together with other Islamist terrorists because the Southern District of New York handled the arrest of the blind Sheikh who was involved in the 1993 World Trade Center bombing. The 9/11 Commission Report, p. 72.).
45 Ibid., p. 82.
46 Ibid., p. 76.
47 Ibid.
48 Ibid., p. 77.
49 Ibid., p. 180.
50 Ibid., p. 79. *The 9/11 Commission Report* also cites reviews conducted in 1999, 2000, and 2001 that concluded information sharing was not occurring as a result.
51 Pluchinsky. According to Pluchinsky, citing U.S. Department of State figures, by 1985 the number of attacks on business-related targets exceeded those on overseas US diplomatic and military facilities combined.
52 Duncan, p. 190.
53 Burton, Fred, *The Terrorism Warning Process: A Look behind the Curtain*, 16 May 2007. Available at: worldview.stratfor.com. The relevance of a warning from an anonymous informant has been questioned by some analysts saying that it was mere coincidence and the product of a fabricator. Coincidence or not, US government officials were warned and the public was not, which clearly created a double standard.
54 *The ‘no double standard’ policy is codified under 49 U.S.C. 44905 and the Department of State’s Statement of Policy in 7 FAM (Foreign Affairs Manual) 052.1.*
56 At the Request of FBI Director Freeh, TIPOFF constructed a parallel system for intelligence officers, nuclear, biological radiological, and chemical proliferators, Russian organized crime and other international crime figures, drug traffickers, alien smugglers, and those engaged in economic espionage. According to TIPOFF figures, by 2004, it had over 10,000 entries. It also inspired a cooperative effort between the CIA and the Department of State to furnish a lookout system for Kenya.
57 In January 2004, John Arriza, TIPOFF’s Director, was praised in Congressional Hearings by the 9/11 Commission for nurturing TIPOFF into the most comprehensive watch list in the U.S. government.
58 *The 9/11 Commission Report*, p. 505. According to TIPOFF statistics: out of a total of 46,358 documents, the CIA was the largest contributor with 16,622, the Department of State next with 15,950, NSA third with 5,752, then FBI with 1,270, and DIA with 728. All other sources, including open-sources, contributed 6,028 documents.
59 Q&As for DCI’s Presentation for 9/11 Inquiry, answer to question 33, 16 May 2002.
60 Ibid., p. 101.
63 Harlow, 2002.
64 Ibid. p. 254 and *The 9/11 Commission Report*, p. 128. In all there were 40 intelligence articles in the *President’s Daily Brief* on bin Laden between 20 January 2001 and 10 September 2001.
66 While Al-Qaeda and its associates killed fewer than 50 Americans in attacks on the US Embassies in Nairobi and Dar es Salaam (1998) and the USS Cole (2000), Hezbollah was responsible for 281 American lives lost in two attacks on the US Embassy Beirut, one on the US Embassy in Kuwait, the bombing of the US Marine barracks in Beirut, the bombing of
the Khobar Towers in Saudi Arabia, and the hijacking of TWA 847. It also was responsible for taking 17 Americans, 15 French, 14 British, 7 Swiss, 7 German, and 27 other hostages during the 1980s in Lebanon.


70 The 9/11 Commission Report, p. 263.

71 On 9/11 TIPOFF contained 1,914 records on Al Qaeda so the reluctance of the CIA to watchlist these particular terrorists was specific. Stranger still, a CTC analyst in August 2001, while reviewing their files, noticed this omission and sent their names to TIPOFF. Unfortunately for the US, the two already had entered the country. Conversation of the author with the analyst. See also: Ibid., p. 270.


73 General John Gordon was made a new Deputy National Security Advisor for Terrorism. Dick Clarke was given Infrastructure Security.


75 The 9/11 Commission Report, 2004, p. 411 ff. Creation of the DNI draws the US closer to British practice – where the Joint Intelligence Committee (JIC) traditionally functions under the chairmanship of a representative of the Foreign and Commonwealth Office who does not directly control collection assets.

76 The first DNI, John Negroponte, was a Senior Foreign Service Officer with extensive experience as an intelligence consumer.


78 See the FBI’s A New Era of National Security, 2001-2008 in which FBI describes its participation on the Matrix and closer cooperation with CIA as part of its response to 9/11. Available at: fbi.gov/history/brief-history/a-new-era-of-national-security

79 The 9/11 Commission lists five analytic centers: CTC, TTIC, DIA, DHS, and FBI and questions whether the US government can afford such duplication in efforts. The 9/11 Commission Report, p. 401.

80 Leiter, Michael, Eight Years after 9/11: Confronting the Terrorist Threat to the Homeland, Statement before the Senate Homeland Security and Governmental Affairs Committee, 30 September 2009.

81 TIPOFF brought over 130,000 names of known or suspected terrorists and the record of over 70,000 ‘hits’ against those names.

82 Fram, Alan, Why can people on the terrorist watchlist buy guns and other FAQs, Associated Press, 14 June 2016.

83 Pistole, John, Deputy Director FBI, address at the George C. Marshall Center. See also: A New Era of National Security, 2001-2008.


85 Intelligence Community/Law Enforcement Community Terrorist Threat Assessment: Current Terrorist Threats to the United States, Community Counterterrorism Board, (U) 26 February 2002.
Law Enforcement Sensitive: Suicide/Homicide Attacker Behaviors – And Suggested Countermeasures, Community Counterterrorism Board, 6 January 2003.

National Terrorism Advisory System, Wikipedia.org.

Australia’s threat system had been stuck for 13 years at medium until raised in 2015 to high by the Prime Minister. Bergin, Anthony and Claire Murphy, ‘Fair Warning: Australia’s terrorist advisories’, The Strategist, Australian Strategic Policy Institute, 16 April 2015.

Homeland Security, NTAS Frequently asked questions. Available at: dhs.gov.


Duncan, p. 191.

Witness the police shooting of the innocent Jean Charles de Mendez in 2005 two weeks after the 7 July 2005 bombings in London on the mistaken assumption that he was another suicide bomber.


Russia is believed to be responsible for these attacks. According to Sergi Markov of the Russian Duma, his aide was responsible for their coordination. Markov said the aid acted on his own and Russia denies any involvement. See: Coalson, Robert, Behind the Estonia Cyberattacks, Radio Free Europe, 6 March 2009.

Bibliography

ACLU, ‘Surveillance under the USA/Patriot Act’. Available at: aclu.org/other/surveillance-under-usapatriot-act.

BBC, “Yemen parcel bomb ‘was 17 minutes from exploding’”, 4 November 2010.

Bergin, Anthony and Murphy, Claire, “Fair Warning: Australia’s terrorist advisories”, The Strategist, Australian Strategic Policy Institute, 16 April 2015.


DCI Counterterrorist Center booklet, June 2002.

Donheiser, Julia, “The United States has spent at least 2.8 trillion on counterterrorism since 9/11,” The Center for Public Integrity, 18 May 2018. Available at: publicintegrity.org.


Fram, Alan, “Why can people on the terrorist watchlist buy guns and other FAQs”, Associated Press, 14 June 1 2016

Gardham, Duncan and McElroy, Damien, “Moscow airport bombing: Russians were warned of imminent attack”, Daily Telegraph, 25 January 2011.


National Terrorism Advisory System, Wikipedia.org.


Q &As for DCI’s Presentation for 9/11 Inquiry, answer to question 33, 16 May 2002


The Department of Justice, *The USA PATRIOT Act: Preserving Life and Liberty*. Available at: justice.gov/archive.


UK Government Response to the Intelligence and Security Committee’s Report into the London Terrorist Attacks on 7 July 2005.

UK Intelligence and Security Committee: *Report into the London Terrorist Attacks on 7 July 2005*.


Further reading

CIA Sherman Kent Center for Intelligence Analysis Papers: Practice of Analytic Tradecraft in the Directorate of Intelligence, Transnational Threats, Profession of Intelligence Analysis, Progressive Management, 2013.
Lowenthal, Mark, M., Ethics of Spying: A Reader for the Intelligence Professional, CQ Press (Congressional Quarterly Press), 2006
Pease, Bruce, Leading Intelligence Analysis: Lessons from the CIA’s Analytic Frontlines, CQ Press, 2019.
Web-based Resources

CIA Freedom of Information Reading Room. Available at: cia.gov/library/readingroom/home.
Department of State, Freedom of Information Reading Room. Available at: https://foia/state.gov/search/search.aspx.
FBI vault. Available at: www.vault.fbi.gov/.
Loyola.edu/dept/politics/intel.html.
Studies in Intelligence at CIA. Available at: https://www.cia.gov/resources/csi/studies-in-intelligence/
Chapter 21


Joshua Sinai

This chapter examines the magnitude of the threat posed by ideologically extremist lone actors who are considered domestic terrorists in the US during the almost 50-year period of the early 1970s to 2019. This should enable us to formulate best practice-based measures to counter them, particularly during the formative pre-incident attack phases. This categorization of terrorist actor types excludes operatives belonging to US or foreign-based organized terrorist groups or their loosely affiliated networks that operate in the US. This is done by outlining the selection criteria for determining the factors that constitute a lone actor terrorist, a listing of significant attacks and plots by a representative sample of 52 perpetrators from the early 1970s to late 2019 (see Appendix A), and, based on these events and how they ended, an assessment of the extremist ideologies and psychological factors that motivated them, their modus operandi, including selection of weaponry and targets, and the measures that will be effective in preventing them during their attacks’ formative pre-incident phases. Also examined is how these incidents and plots were resolved, particularly the measures used in preventing the ones that had failed to be executed. Several security technologies that are being employed to counter such perpetrators’ pre-incident suspicious activities are also discussed. As an empirical study, the statistically-based findings are based on the chapter’s database of actual cases during the almost 50-years that are covered. The conclusion presents the chapter’s overall findings.

Keywords: lone actor/lone wolf, terrorism, radicalization, modus operandi, target selection, preemption, prevention.
Violent attacks by lone actor terrorists are a relatively frequent occurrence in the US. While a minority of terrorist incidents in the US are committed by members of organized terrorist groups or loosely affiliated networks, the majority are conducted by lone actors. This chapter focuses on terrorist attacks by ideologically extremist lone actors who are domestic terrorists - not operatives belonging to organized terrorist groups or their loosely affiliated networks in the US - during the almost 50-year period of the early 1970s to 2019. Significant examples of lone actor attacks include the shooting rampage by ISIS adherent (but not member) Omar Mateen at the Pulse Nightclub in Orlando, Florida, on 12 June 2016, (49 killed, 53 wounded); the late October 2018 mailings of more than a dozen homemade package bombs by the far-rightist militant Cesar Sayoc against his perceived politically liberal adversaries, including the broadcast network CNN (no casualties, but mass disruption); and the shooting rampage by the virulently anti-Semitic Robert Bowers against congregants at the Tree of Life synagogue in Pittsburgh, Pennsylvania, on 27 October 2018 (11 killed and six wounded). In another mass shooting by a lone actor terrorist, on 3 August 2019 Patrick Crusius killed 22 people and wounded 24 others in his white supremacist- and anti-immigration-influenced attack at a Walmart department store in El Paso, Texas.

This chapter’s objective is to examine the magnitude of the threat posed by lone actor terrorists in the US and to discuss measures required to prevent such attackers during the pre-incident phases, if possible. This is done by outlining the selection criteria for determining the factors that constitute a lone actor terrorist, a listing of significant attacks and plots by a representative sample of 52 perpetrators from the early 1970s to late 2019 (see Appendix A), and, based on these events and how they ended, an assessment of the extremist ideologies and psychological factors that motivated them, their modus operandi, and the measures used by the US government and others to preempt them during their attacks’ formative pre-incident phases. Some security technologies that are being employed to counter their pre-incident suspicious activities are also discussed. The conclusion presents the chapter’s findings.

By coincidence, as this chapter’s research was being completed in November 2019, the Federal Bureau of Investigation (FBI) published Lone Offender: A Study of Lone Offender Terrorism in the United States, 1972-2015. Like this chapter, the FBI’s report also presents statistical findings on 52 cases of lone actor terrorist events and plots during a comparable period. However, unlike this chapter, specific information about the identity of the FBI’s 52 cases is not presented, likely due to the legal sensitivity of revealing such information by a criminal investigatory agency. It is likely, therefore, that some of the incidents listed in this article might not be included in the FBI’s study and vice versa. Nevertheless, the FBI’s study is methodologically relevant and authoritative, so its inductive-based statistical findings are compared to this chapter’s deductive-based findings for purposes of comparison. On some issues that were beyond the capability of the present study, the FBI study’s findings are presented.

Selection Criteria

Several criteria were selected to examine lone actor terrorists in the US. These include the timeline for the representative sample chosen, their role as domestic (US) actors, whether domestic and/or foreign-based ideologies apply, and, finally, to qualify for inclusion, one of the attackers must be the attack’s primary architect and actor.

First, the almost 50-year period of the early 1970s to late 2019 was selected because it presents a manageable timeframe to generate generalizable inferences about a spectrum of trends concerning lone actor terrorists.

In the second criterion, the selected violent lone actors had plotted, attempted or completed a terrorism-motivated attack in the US. Although numerous violent lone actors in the US commit mass fatality attacks, for this chapter only ideologically driven terrorists were selected,
as opposed to what are termed psychologically-disordered active shooters. This is not intended to imply that some ideologically-driven terrorists are not considered psychologically-disordered individuals as well, but that being driven by extremist ideologies is the primary distinguishing characteristic of such violent perpetrators. For this reason, neither Aaron Alexis’s shooting rampage at the Washington, DC, Navy Yard (16 September 2013), nor Stephen Paddock’s mass shooting in Las Vegas, Nevada (1 October 2017) were included because a terrorist motivation had not been proven as a motivating factor for their attacks.

In the third selection criteria, the lone actors are categorized as domestic terrorists. In this chapter, domestic terrorism is defined broadly to include persons who attack other Americans for political objectives, while such perpetrators reside in the US at the time of their attack, whether as citizens or on visitors’ visa. As part of this geographical-based criterion, such lone actors are considered homegrown terrorists, as opposed to “one-person” foreign-based terrorists who are deployed by a foreign terrorist organization to conduct an attack in the US. For this reason, foreign-deployed “single terrorists” are not included, such as British national Richard Reid (22 December 2001) or Nigerian national Umar Farouk Abdulmutallab (25 December 2009) who both tried to explode aircrafts approaching US airports.

Similarly, several US homegrown high-profile terrorist operatives such as Adam Gadhan, Anwar al-Awlaki, Najibulla Zazi, Samir Khan, and Omar Shafik Hammami (AKA Abu Mansoor al-Amraki) are also not included in the listing of lone actors because they had travelled overseas to join foreign terrorist groups. On the other hand, Khalid Aldawsari, a Saudi Arabian national, who was studying in the US on an expired student visa, who was arrested for plotting an attack in Dallas, Texas, in February 2011, qualified for inclusion because he was already residing in the US at the time of his plot.

As to the fourth criterion, to qualify as domestic terrorists the extremist ideologies motivating them are either US, or foreign-based (or a combination of the two): this definition does not represent any government definition, as the US, at least as of late 2019, had not legislated an official definition of domestic terrorism that addresses both domestic- and foreign-based ideologies as motivation, but is this author’s own definition, at least until a relevant definition is officially agreed upon. Generally, the extremist ideologies motivating domestic terrorists are primarily far-right-wing, far-left-wing, or Islamist. The far-right-wing groups that inspire vulnerable persons include white supremacists, neo-Nazis, Christian Identity, sovereign citizens movement, anti-abortionists, and others. The far-left wing ideologies that motivate them include extremist environmentalists (including anti-modern technology), anti-law enforcement, anti-globalists, and others. In a few cases, the extremist ideologies driving such lone actors are a blend of confused conspiratorial anti-government libertarianism that cannot be characterized as either far-right-wing or far-left-wing.

Fifth, the status of “loner” makes such perpetrators unique as opposed to being members of organized terrorist groups or loosely affiliated networks. This is particularly the case due to their lack of training, provision of weapons, and other forms of logistical support by organized terrorist groups at the time of their plots or attacks, although several such perpetrators underwent military training during their military service in the US (such as Timothy McVeigh, Oklahoma, 19 April 1995). Their status as “lone,” however, does not imply that they must be single actors, although it is the case that most lone actors are single perpetrators. As explained by the FBI’s study, to qualify as lone actors, if two perpetrators are involved, one of them must have been the primary architect and actor in the attack.

Defining lone actors has been the subject of controversy in academic literature. As Hamm and Spaaij write, “Some experts use an expansive definition of lone wolf terrorism in terms of both motives and the number of perpetrators involved.” They cite Jeffrey Simon’s definition as “the use or threat of violence or nonviolent sabotage, including cyber-attacks, against government, society, business, the military … or any other target, by an individual acting alone or with minimal support from one or two other people … to further a political, social, religious,
financial, or other related goal," to create fear and disruption that provokes heightened government reaction.

With a consensual definition of what constitutes lone actor terrorists still in contention, this chapter accepts the definitions by Simon and the FBI that lone actors can cooperate with one or two other individuals as long as one of them is the primary attack perpetrator, that they are not directly linked to an organized terrorist group, and that they self-fund and self-weaponize their operations, including during the plot phase. As examples, the cases of a husband-and-wife mass shooters (San Bernardino, California, 2 December 2015) and two brothers (Boston Marathon, 13 April 2013) are included because they acted as “joint” actors and exhibited the characteristics of a lone actor terrorist by having no direct affiliation with a foreign terrorist group. Also, Timothy McVeigh is included because he was the primary perpetrator of the Oklahoma City bombing (19 April 1995), with Terry Nichols, his main collaborator, playing a secondary role. In all these cases, there were no direct ties to any organized militant group.

In another component of defining such violent individual actors, this chapter terms them as “lone actors” as opposed to “lone wolves” (which is used by numerous studies) because, as Bart Schuurman, et al, point out, the “latter implies a high level of cunning and lethality that is often not present among” such perpetrators.

Assessment

The chronology involving 52 incidents listed in the Appendix is intended to serve as a representative sample as opposed to a complete listing of every case of lone actor terrorist attacks (or plots) over the past 50 years in the United States. As such, it is intended to provide a preliminary basis to generate six primary objectives. The first objective is to provide an empirical baseline to identify trends in the frequency of lone actor terrorist incidents over a 50-year period, allowing us to determine whether it is on the rise or in decline. With lone actors defined broadly to include two-persons (e.g., brothers or husband and wife) in some incidents, the second objective is to identify the prevalence of the two-person lone actor teams among the overall sample. The third objective is to identify the lone actors’ gender. The fourth objective is to ascertain some of the psychological factors that might drive susceptible individuals into becoming lone actor terrorists. The fifth objective examines the types of ideologies that motivate such perpetrators. The sixth objective is to examine trends in modus operandi among the lone actor terrorists, such as their selection of weaponry and targets. The final objective is to identify how these incidents and plots were resolved, particularly the measures used in preventing the ones that had failed to be executed. It is hoped that examining the outputs of these objectives will generate findings on best practices in preventing such incidents.


In terms of rates of incident trends, there has been a substantial increase in the number of plots and attacks over the years, with an especially heightened increase since the early 2000s. This is demonstrated by Table 1.

Based on these data, there was a dramatic escalation in the frequency of lone actor terrorist attacks and plots over the years (see Figure 1). This was especially the case during the period of 2010 to 2019, with the largest number of incidents (attacks (successful or not, and plots) (N=30, 71.4 per cent) and plots (N=8, 80 per cent). It should be noted that Ted Kaczynski’s mail bomb attacks lasted from the 1970s into the 1980s, but they are counted as one attack in the 1970s. Of special concern is that since 2015 there have been 17 attacks (N=17, 40.4 per
cent), the largest number of attacks during a five-year period since the early 1970s, indicating a heightened state of political and social polarization in American society.

Table 1. Trends in frequency of lone actor terrorist incidents 1970-2019

<table>
<thead>
<tr>
<th>Decade</th>
<th>Incidents</th>
<th>Attacks</th>
<th>Plots</th>
<th>Plot Detail</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1970-1979</td>
<td>Beginning of the Unabomber package bomb attacks</td>
<td>2</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1980-1989</td>
<td>No significant incident except for continuation of Kaczynski’s mail bomb attacks</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1970-2019</td>
<td></td>
<td>42</td>
<td>10</td>
<td>10</td>
<td>52</td>
</tr>
</tbody>
</table>

Figure 1. Lone Actor Attack Incidents by Decades showing Attacks and Plots
2. Prevalence of One over Two-person Lone Actors

Of the 52 attacks and plots, the two-person teams who qualified as “lone actors” consisted of Timothy McVeigh and Terry Nichols (April 1995), John Allen Muhammad and Lee Malvo (October 2002), Abu Khalid Abdul-Latif and Walli Mujahidh (December 2011), Tamerland Tsarnaev and Dzokhar Tsarnaev (April 2013), and Syed Rizwan Farook and Tashfeen Malik (December 2015). Their four attacks constituted 9.4 per cent of the total attacks, and their single plot constituted 10 per cent of the total plots.

3. Gender

In this sample, the overwhelming gender of the attackers was male, with only one female participating in an attack with her husband in an attack (San Bernardino, December 2015). This may be explained, at least in the case of the US, by the preference of radicalized females to join organized terrorist groups because these provide them with a sense of belonging to a community, as opposed to engaging in lone actor-type attacks.11

4. Psychological Drivers

In terms of their psychological drivers, according to the literature, the individuals who choose to become lone actor terrorists do so because they prefer not to be “formally involved with terrorist networks that would have happily given guidance and material support.”12 With many of these perpetrators being probably frustrated with their personal lives, (e.g. being unmarried), as well as being frustrated with their professional lives (e.g. lacking a steady job), joining militant groups would represent a way out. However, paradoxically, with their failure to even fit into such groups because of their difficulty in getting along with other members due to their “social ineptitude” and other psychological factors, they therefore become isolated lone actor attackers.13 This was the case with Timothy McVeigh and Terry Nichols, the perpetrators of the bombing of the Alfred P. Murrah Federal Building in Oklahoma City (19 April 1995) who were “ostracized by the Michigan Militia because they advocated … violence.”14 With regard to several lone actor terrorists who were married, while each appeared to be motivated by different psychological drivers, they shared certain commonalities. In the case of husband-and-wife Syed Rizwan Farook and Tashfeen Malik (December 2015) and Omar Mateen (June 2016), even though each was married and had infant children, they appeared to have self-radicalized themselves into violent extremism to such an extent that they had become desensitized to the consequences of their violent attacks on the fate of their children and families.15

In a related psychological driver, several of the lone actor terrorists had a history of engaging in domestic violence. With men being the overwhelming majority of attackers, as Joan Smith explains, such perpetrators share a sense of perverse entitlement that causes them to “seek to control every aspect of the lives of their wives and children” without any interest in “considering their long-term welfare” or “protecting them from the consequences of [their] horrific public acts of violence. It is a chilling view of family relationships in which becoming a husband and father appears to have more to do with confirming a man’s status … than forming close attachments.”16 Examples of lone actor terrorists who reportedly had abused their wives or girlfriends include Faisal Shahzad (May 2010),17 Tamerland Tsarnaev (April
2013), Robert Lewis Dear Jr. (November 2015), Omar Mateen (June 2016), Cesar Sayoc Jr. (October 2018), and others.

5. Ideological Motivations

In this study’s sample of 52 cases, five of the perpetrators appeared to be motivated by more than one extremist ideology, so a total of 57 ideological views are considered. Of these, Jihadism was most prevalent (N=25, 43.8 per cent), followed by white supremacy/Neo-Nazi (N=12, 21.0 per cent), anti-Jewish (N=7, 12.2 per cent), anti-government (N=6, 10.5 per cent), anti-abortion (N=2, 3.5 per cent), anti-gay (N=1, 1.7 per cent), survivalist (N=1, 1.7 per cent), anti-technology (N=1, 1.7 per cent), promoting anthrax (N=1, 1.7 per cent), and what can be considered as an amalgamation of conspiracy theories (N=1, 1.7 per cent) (see Figure 2).

![Figure 2. Ideologies Motivating Lone Actor Attacks in the United States, 1970s – 2019](image)

6. Modus Operandi: Tactics, Weapons and Target Selection

Lone actor terrorists employed a variety of tactics, weapons, and targeting.

**Tactics**

In terms of tactics, out of the 52 attacks, nine involved serial attacks (21.4 per cent). With four of the nine serial attacks occurring in the 2010-2019 period, such tactics are expected to continue to be used by lone actor terrorists. Serial killing attacks are defined as involving “a temporal separation between the different murders” by a single perpetrator, characterized by a distinctive time period between the murders, with “cooling-off” periods. Note that attacks where the attackers manage to escape but continue their attack are not considered as serial attacks.
With regard to employment of weapons, 57 weapons were used in the 52 incidents, with five of the perpetrators employing two different weapons in their attacks. Of the 57 weapons, firearms accounted for almost half (N=28, 49.1 per cent), bombs for almost one quarter (N=14, 24.5 per cent), with the remainder accounting, with the exception of vehicle bombs, for less than 5 per cent each: package bombs (N=2, 3.5 per cent), anthrax letters (N=1, 1.7 per cent), ricin letters (N=2, 3.5 per cent), aircraft (N=1, 1.7 per cent), vehicle bomb (N=3, 5.2 per cent), vehicle ramming (N=3, 5.2 per cent), knife (N=1, 1.7 per cent), drone (N=1, 1.7 per cent), grenade (N=1, 1.7 per cent). In five of the incidents, three firearms and bombs were employed, in one a firearm and grenade, while one involved vehicle ramming and a knife. The distribution of incidents by weapon type and decade are shown in Figure 3.

As Figure 3 shows, the relative use of firearms had increased since the 1990s. The overall number of lone actor attack incidents has increased significantly as well over the entire period covered by this study.

For comparison purposes, in the FBI’s lone offender study (N =52), firearms also were the most common type of weapon (n=35, 67 per cent), followed by bomb explosives (n=14, 27 per cent), bladed instruments (knives) (4 per cent), vehicles/airplane (6 per cent). Based on these two databases, the overwhelming majority of weapons used or intended to be used in these attacks were low-tech. The single high-tech weapon employed in an attack was anthrax. With Bruce Ivins, the single actor perpetrator who was viewed as the alleged sender of the anthrax letters working at a biodefense laboratory, it can be hypothesized that for lone actor perpetrators of such high-tech attacks, it would be necessary for them to be insiders or otherwise associated with sophisticated laboratories in order to produce such weaponized bio-agents.

In terms of the target selection for the attacks and plots in the 52 incidents, several attacks included two or three targets, bringing the total of target types to 66 (see Figure 4). Targeting public areas was predominant (N=16, 24.2 per cent), followed by military facilities/personnel (N=14, 21.2 per cent), public/government figures (N=7, 10.6 per cent); faith-based
organizations (FBOs) (N=6, 9.0 per cent), government facilities (N=5, 7.5 per cent), airports (N=3, 4.5 per cent), colleges/ universities (N=3, 4.5 per cent), sports events (N=3, 4.5 per cent), abortion clinics (N=2, 3.0 per cent), nightclubs (N=2, 3.0 per cent), office buildings (N=1, 1.5 per cent), retail stores (N=1, 1.5 per cent), transportation (N=1, 1.5 per cent), and media (N=2, 3.0 per cent).

7. Resolution of Plots and Incidents
The 52 incidents were resolved in several ways. First, 42 attacks were executed by the attackers, with one of them, an attempted vehicular bombing in Times Square, failing to explode (May 2010). Second, of the 38 attacks carried out by single attackers, 26 of the perpetrators were arrested following their incident (68.4 per cent); eight were killed in a shootout following their attack (21.0 per cent), with one killed when the bomb exploded in his vehicle; and three committed suicide at the scene of their attack (7.8 per cent). Third, in the four attacks that involved two attackers, five were arrested and three were killed in a shootout.

Figure 4. Targets by Number of Incidents (Plots and Attacks)
Fourth, of the 52 incidents, 10 (19.2 percent) involved plots that were thwarted through US government’s law enforcement undercover preemption by the arrest of the alleged perpetrators.

**Preventing Lone Actor Terrorist Attacks**

Based on this study’s seven objectives breakdown of the magnitude of the threats posed by lone actor terrorists in the 52 incidents, half a dozen generalizable findings highlight measures that could preempt and prevent such attacks during their pre-incident preparatory phases.

First, when it comes to preventative measures, it is important to be aware of the nature of the lone actor terrorists in order to prepare to defend against them with appropriate response measures. Based on the 52 incidents, the lone actors are likely to be males, with a majority of the operatives attacking alone, although it is still possible for some of the attackers to be two-person “lone actors,” with one of them the primary attacker. Also, in their modus operandi, the weapons chosen are likely to be low-tech firearms, followed by bombs. However, one should also anticipate other weapons to be employed such as vehicles, weaponized letters/packages, knives, and drones. As demonstrated by the 2001 anthrax letter attacks, however, even a single lone actor may be capable of developing certain types of high-tech weapons. Therefore, these types of sophisticated weapons need to be considered as well in formulating threat assessments of the types of weapons possibly to be employed by them. At the same time, their targets are still likely to be primarily public spaces, followed by military facilities and personnel, public and government officials, faith-based organizations (FBOs), colleges/universities, and transportation facilities such as airports.

There are a number of important findings from analyzing the relationships of the various data fields developed for this study, particularly for more effectively preventing attacks by lone actor terrorists based on the types of tactics, weapons, and targets. The study also developed a measure of relative death and injury consequences per attack that provides insight into response measures that might show the greatest impact relative to the level of effort/cost, and therefore, a rough return on investment (ROI).

It is important for counter-terrorism, law enforcement, and infrastructural protection agencies, therefore, to prioritize their response measures to upgrade the defensive posture of the facilities most at risk of being attacked by lone actor terrorists.

Second, it is crucial to identify such perpetrators’ pre-incident suspicious behaviors and mindsets. This can provide early warning indicators that a suspect might be transitioning through a trajectory from hateful on- and off-line utterances to terrorist activity. This is confirmed by the FBI’s lone offender study, which concluded that “prior research and operational experience support the conclusion that acts of targeted violence, including lone offender terrorist attacks, may be preventable through early recognition and reporting of concerning behavior.” As explained by the FBI’s study, early warning observables about such individuals that can lead to preemptive intervention need to be noticed by bystanders, such as family members; peers such as co-workers, classmates, friends and acquaintances; employers, mental health professionals, religious leaders, and law enforcement officers; and even “strangers,” such as vendors who sell them precursor materials or weapons, including observing their suspicious behavior in “online or offline public spaces.”

Although detailed information about how the ten plots were foiled is not publicly available, it can be assumed that their perpetrators’ early warning observables likely led to bystanders’ informing their suspicions to law enforcement authorities for early preemption. Such awareness by bystanders is so important because at least two significant mass shooting attacks among the 42 cases could have been prevented if their perpetrators’ extremist views had been reported by their workplace colleagues to appropriate authorities. This was the case with Major Nidal Hasan (November 2009) and with Farook (December 2015), whose extremist views were known to their colleagues. In the case of Farook and his wife, neighbors in their apartment
building had also noticed their stockpiling of weapons. While viewed in isolation, such concerning activities might not have indicated potential terrorist activity, once correlated with each other, they indicated a high risk of becoming a violent insider threat to their fellow workers. When such early warning signs become noticeable to fellow co-workers and supervisors, they need to be reported to appropriate authorities for preemptive response. As the DHS motto states: “when you see something, say something.”

Third, the need for early preemption of such perpetrators makes it crucial for law enforcement authorities to employ the practice of stings against them. As explained by Oroszi and Ellis, the FBI, which is the lead agency in investigating acts of terrorism in the US, will in such cases receive a tip from a “bystander” who might notice a susceptible individual’s expression of extremist beliefs, whether in social media or in person, that might indicate an imminent trajectory into violence, this would be followed by the deployment of an undercover agent or informant to befriend them. The FBI would arrange a sting in which the potential terrorist would have the opportunity to attempt to carry out an operation, such as detonating a bomb supplied to them. This practice is justified, Oroszi and Ellis argue, because “if the person shows a predisposition toward perpetrating the crime, ultimately chooses the crime and the target, and takes steps toward accomplishing the infraction, then they were not entrapped, they were caught.”

Fourth, several of the study’s perpetrators had been previously incarcerated for criminal activity. They were radicalized into extremism while in prison, and turned to terrorism following their release. In such cases, it is the responsibility of their parole bodies to continue watching them during their post-release phase to ensure they do not proceed to engage in terrorist violence. In the FBI study, for example, 35 offenders (70 per cent) were arrested at least once as an adult before their attack. With such lone actors likely to self-fund their terrorist attacks, law enforcement authorities need to be aware how such criminal activities, most of which, when viewed singly on their own may not necessarily indicate a link to terrorism, but that when such operatives are identified as motivated by an extremist ideology such a correlation will likely point to a nexus to a potential terrorist attack. It is at this point that these warning indicators represent the probable establishment of a seedbed for a lone actor or cell activity in that locality, thus warranting the activation of a counterterrorism target-zone investigation.

Fifth, in another preventative measure, the case of lone actors who conduct mailed letter or package bomb campaigns, advances in detection technologies now make it more likely to identify them for arrest. This was not the case when Ted Kaczynski had embarked on his weaponized package mailing spree from May 1978 to April 1995, with a single tip by his brother leading to his arrest. In the current period, technological advances in biometric fingerprint and DNA detection of such senders, including the automated capability to digitally reverse engineer the transport movement of mailed letters and packages, now make it possible for law enforcement authorities to quickly identify and apprehend such threat actors. This was the case with Cesar Sayoc, Jr., who was identified and arrested as a possible suspect within days of the biometric identification of his weaponized packages.

Sixth, a useful preventative methodology to forecast the likelihood of individuals who demonstrate a susceptibility into becoming lone actor terrorists is to apply pathways to violence (PTV) models to map their possible trajectories into violence. In these PTV models, a trajectory into violence is outlined into distinct pre-incident phases, such as triggers (a traumatic event, such as personal, professional, and ideological crises), ideation/fantasy (thinking about taking revenge of some sort to avenge a perceived grievance, including being driven by an extremist ideology), crossing a threshold into preparatory activities (such as acquiring weapons/ammunition), and approaching a target to conduct an attack. Once such early warning indicators are noticed, for instance, by an organization’s threat assessment team, these signs
need to be aggregated to form a risk score (such as low, medium, or high) for appropriate intervention and mitigation, whether by mental health counselors or law enforcement agencies.

Finally, the radicalization of susceptible individuals into becoming lone actor terrorists can be preempted through various preventative community-level approaches. These would include providing vulnerable subjects appropriate programs that would promote peaceful alternatives to the pursuit of violence to fulfill their objectives by providing them with a sense of belonging and giving a new meaning to their lives.27 This is important “because the best way to stop terrorism is by preventing its causes.”28

Dr. Joshua Sinai is a Professor of Practice in Counterterrorism Studies at Capitol Technology University, in Laurel, Maryland, USA. He also teaches a graduate-level distance learning course on “Global Terrorism” at Southern New Hampshire University’s Criminal Justice Department. He has more than 30 years of professional experience in terrorism and counterterrorism studies in the U.S. Government, academia, and the private sector. He specializes in analyzing and mitigating what is termed “active threats”: terrorism, active shooters, workplace violence, and “insiders”. A widely published author, his publications include “Active Shooter: A Handbook on Prevention” (ASIS International, May 2016, 2nd edition); a chapter on “The United States of America’s Domestic Counterterrorism Since 9/11,” in: Andrew Silke (ed.), “Routledge Handbook of Terrorism and Counterterrorism” (Routledge, 2018); and a chapter on “Israel and Combating Terrorism: Assessing the Effectiveness of Netanyahu’s Combating Terrorism Strategy”, in Robert O. Freedman (ed.), “Israel Under Netanyahu: Domestic Politics and Foreign Policy” (Routledge, 2020). As a veteran book reviewer, he serves as Book Reviews Editor of the online journal Perspectives on Terrorism, for which he also writes the “Counterterrorism Bookshelf” review column. He earned his Master’s degree and PhD from Columbia University in Political Science.

Acknowledgment
The author would like to thank Jeffrey Fuller, President of Security Risk, Inc., for peer reviewing this chapter and for developing and operationalizing an algorithm that made it possible for incident and perpetrator data in the Excel Spreadsheet to generate the study’s statistical findings.
Appendix: 52 Significant US Incidents, 1970s to 2019

To generate the chapter’s findings, 52 significant incidents involving lone actor terrorists were selected covering the period from the early 1970s to late 2019.

6 August to 20 August 1974: On 6 August 1974, Muharem Kurbegovic, 31, a Yugoslavian immigrant, set off a homemade bomb at Los Angeles International Airport, killing three people and wounding 36 others. In his more than two week-long bombing spree, he also firebombed the houses of a judge and two police commissioners, as well as one of the commissioner’s cars. He also burned down two Marina Del Rey apartment buildings and threatened Los Angeles with a gas attack. He was nicknamed “The Alphabet Bomber” because of his alleged plan to attack places in an order that would make an anagram of Aliens of America. “A” for airport, “L” for locker, etc.29 With his announcements to the media about his forthcoming bombings, which created large-scale panic in the city, a 1,000-man Los Angeles Police Department (LAPD) task force was established to apprehend him.30 He was arrested on 20 August 1974. He stood trial in 1980 and was sentenced to life in prison. He claimed his motivation was to “undermine and erode the foundation of Western Civilization, which is the Holy Bible.”31

25 May 1978 to 24 April 1995: Ted Kaczynski, known as the “Unabomber,” 36-year-old at the start of his attacks, conducted a mail package bombing campaign, which killed three people and wounded 23 others. Nine of the 16 known package bombs were delivered via the mail service to target universities, airlines, and newspapers.32 Kaczynski was a former university professor of mathematics turned environmentalist anarchist, who believed that his bombings were necessary to call attention to how modern technologies and scientific research have destabilized society, increased psychological suffering, and eroded human freedom. While still on the loose, a break in the case occurred when, in cooperation with authorities, the New York Times and Washington Post published Kaczynski’s diatribe against technological advancement (known as the “Unabomber Manifesto”) on 19 September 1995, in exchange for an end to his violence. It was at that time that David Kaczynski recognized the manifesto as his brother’s writing and notified law enforcement authorities. This led to the FBI-ATF task force’s eventual identification of his cabin in Montana, leading to his arrest on 3 April 1996.33 On 22 January 1996 Kaczynski accepted a plea agreement sentencing him to life imprisonment without parole.

25 January 1993: Mir Aimal Kansi, 29 (or 34), carried out a shooting spree against vehicles waiting at a red traffic light to make a left turn into the main entrance of the CIA Headquarters in McLean, Virginia. Two people were killed and three others were wounded. Kansi then returned to his vehicle, and after arriving at his apartment in Reston, Virginia, booked a flight to Pakistan, his home country. On 15 June 1997, he was arrested by a team of FBI officers at his hotel room in Dera Ghazi Khan in the Punjab province, and extradited to the US Following his trial in the US, he was sentenced to death. Kansi had entered the US in 1991, using forged papers under his assumed name, which also enabled him to purchase a fake US green card. Reportedly, his motivation for the attack was a desire to punish the US government for bombing Iraq, its involvement in the killing of Palestinians, and the involvement of the CIA in the internal affairs of Muslim countries.34

19 April 1995: Timothy McVeigh, 26, drove a bomb-laden truck to the front of the Alfred P. Murrah Federal Building, Oklahoma City, Oklahoma, and detonated a fuse setting off an explosion that destroyed the northside of the building. The explosion killed 168 people, and wounded 684 others. A Gulf War army veteran, McVeigh reportedly sought revenge against what he regarded as a tyrannical federal government that was responsible for several incidents involving the deaths of far-right militants. He was arrested shortly after the bombing, indicted on 160 state offenses and 11 federal offenses, including the use of a weapon of mass destruction. He was found guilty on all counts in 1997 and, after being sentenced to death, was
executed on 11 June 2001. Two of his fellow conspirators in the plot, Terry Nichols, 40, and Michael Fortier, 26, were also arrested and sentenced to long-term imprisonment, with Nichols playing an operational role in helping to build the explosive device.

27 July 1996 to 29 January 1998: Eric Robert Rudolph, 29, a Christian Identity White Supremacist, began conducting a series of bombings, including at the 1996 Summer Olympics, Atlanta, Georgia, abortion clinics, and a gay bar in Atlanta. These bombings killed three people and wounded 150 others. Becoming a fugitive, he was arrested in Murphy, North Carolina, on 31 May 2003. On 8 April 2005, Rudolph agreed to a plea deal to plead guilty on all charges in exchange for life imprisonment.

18 September to 15 October 2001: In the immediate aftermath of Al-Qaeda’s 9/11 attacks, a batch of several letters containing anthrax bacterial spores were dropped at a mailbox in Princeton, New Jersey. Two letters, which reportedly contained a potent form of Bacillus anthracis (the causative agent of anthrax), arrived at the offices of Senators Tom Daschle and Patrick Leahy on 15 October. Letters were also sent to the offices of news organizations and US Congressional lawmakers. The attacks infected 22 persons, with five of them dying as a consequence. Several additional copycat hoax letters were reportedly sent by others. During the course of a seven-year investigation by the FBI it was concluded that Bruce Ivins, 56, a senior biodefense researcher who had worked with Bacillus anthracis at the US Army Medical Research Institute of Infectious Diseases (USAMRIID) in Frederick, Maryland, was the “sole perpetrator of the anthrax attacks.” The motive for the letter attacks had also not been conclusively proven, with one possibility being that Ivins may have viewed the letters’ lethal impact as an opportunity to rejuvenate interest in his anthrax vaccine program that was facing closure. He committed suicide in July 2008 (reportedly fearing that he was about to be arrested).

2 July 2002: Hesham Mohamed Hadayet, 41, opened fire at the airline ticket counter of El Al, Israel’s national airline, at Los Angeles International Airport, California. Two people were killed and four others were wounded. Hadayet was fatally shot by an El Al security guard. Hadayet, an Egyptian national, had a green card which allowed him to work as a limousine driver. He was married (with a child) and was living in Irvine, California.

October 2002: In what became known as the “DC Sniper Attacks” or the “Beltway Sniper Attacks,” over a three weeks long period, John Allen Muhammad, 41, and Lee Boyd Malvo, 17, used their 1990 Chevrolet Caprice sedan to launch a series of coordinated sniper attacks in Maryland and Virginia. Ten people were killed and three others were wounded. Their murderous spree included armed robberies in several other states that resulted in seven deaths, with seven others wounded. After being captured and arrested, Muhammad was sentenced to death in September 2003, while Malvo was sentenced to six consecutive life sentences without parole. As one of the motivations for the shooting spree, it was reported that Muhammad - who was born as John Allen Williams and had converted to Islam in 1987 when he joined the Nation of Islam - had written jihadi diatribes against the US, with his ultimate goal to “shut things down” across the US.

28 July 2006: Naveed Afzal Haq, 30, carried out a shooting attack at the Jewish Federation of Greater Seattle building, Seattle, Washington, killing one person and wounding five others. During the incident, Haq called 911, telling the operators that “These are Jews and I’m tired of getting pushed around and our people getting pushed around by the situation in the Middle East.” He also demanded that the US withdraw its military forces from Iraq. When he walked out of the building with his hands on his head he was arrested by the police. On 15 December 2009 he was found guilty on all counts, including aggravated first-degree murder, and was sentenced to life without parole plus 120 years.

1 June 2009: Carlos Bledsoe (aka Abdullahkim Mujahid Muhammad), 23, carried out a drive-by shooting attack on US Army soldiers in front of a US military recruiting office in Little Rock, Arkansas, killing one soldier and wounding another. He drove away from the
scene, but was captured by the pursuing police. A convert to Islam, he had gone to Yemen in 2007 to teach English, but after overstaying his visa was deported to the US. He had claimed he was acting on behalf of Al-Qaeda in the Arabian Peninsula (AQAP), but it was likely he was motivated by its ideology. He was also considered to have personal problems.

10 June 2009: James Wenner von Brunn, 88, a White Supremacist and Neo-Nazi, carried out a shooting attack at the US Holocaust Museum, in Washington, DC, killing Stephen Tyrone Johns, a Museum Special Police Officer. With other security guards returning fire, von Brunn was wounded and then arrested. On 6 January 2010, von Brunn died of natural causes while awaiting trial.

24 September 2009: Michael C. Finton, 29, a convert to Islam known as Talib Islam, was arrested by the FBI for plotting to bomb the Paul Findley Federal Building and the adjacent offices of Congressman Aaron Schock, in downtown Springfield, Illinois. After pleading guilty in a federal court on 9 May 2011, he was sentenced to 28 years’ imprisonment. Finton was arrested by an FBI undercover agent who was posing as an Al-Qaeda operative.

24 September 2009: Hosam Maher Husein Smadi, 19, a Jordanian citizen staying in the US on an expired 2007 visa, was arrested by the FBI for plotting to bomb Fountain Place, a tall building in Dallas, Texas. Coming under FBI radar for his suspicious activities, Smadi had been placed under continuous surveillance, including entrapping him into believing he was involved with an Al-Qaeda sleeper cell that was supplying him with chemicals for a bomb explosive. On 20 October 2010, he was sentenced to 24 years’ imprisonment.

5 November 2009: Major Nidal Hasan, 39, a US Army Medical Corps psychiatrist, carried out a shooting rampage at his military base in Fort Hood, Texas, killing 13 people and wounding more than 30 others. At the end of his attack, he was wounded by the responding police, as he gave himself up. In August 2013 he was convicted in a court martial and sentenced to death. Numerous early warning red flags were missed by US government and military authorities prior to Major Hassan’s shooting rampage. First, in 2007, at his fellowship program at the military’s medical school, the Uniformed Services University of the Health Sciences, in Bethesda, Maryland, Major Hassan’s supervisors reportedly were “‘derelict in their duties” by failing to take “appropriate action” against him by reporting to the base’s security officer his extremist Islamist statements in class and to his student colleagues.”

Secondly, Major Hasan’s more than several dozen email exchanges in December 2008, and January and May 2009 with Anwar al-Awlaki, a prominent Al-Qaeda cleric (and, reportedly, an operational planner, as well) based in Yemen, were known to the FBI’s Joint Terrorism Task Force (JTTF) in San Diego, California, which was tracking Awlaki’s communications at the time.

Although Major Hasan was on active military duty and was listed as a “Comm Officer” at the Walter Reed Army Medical Center in Washington, DC, this email exchange was considered to constitute ‘academic research on Islamic beliefs regarding military service’, but not sufficiently suspicious to raise warning flags of a possible radicalization that could lead to a terrorist attack. Finally, after Major Hasan was transferred to Fort Hood in June 2009, where he was responsible for counseling soldiers returning from Iraq and Afghanistan, he purchased an FN Herstal semi-automatic tactical pistol and ammunition at the Guns Galore gun store in Killeen, Texas. At the time, this did not raise any suspicions with the FBI background check that was conducted under the National Instant Background Check System when Major Hasan purchased the pistol. However, a suspicion would have been raised if that information had been shared with the JTTF in Washington, DC, which was also tracking him and was aware that he had repeatedly contacted Anwar al Awlaki over the internet. Reportedly, when Major Hasan was informed in October that he would be deployed to Afghanistan it triggered the set of risky behaviors that led to his walking into a deployment processing center at Fort Hood on 5 November 2009 to conduct his shooting rampage against his fellow soldiers.

18 February 2010: Andrew Joseph Stack III, 53, deliberately crashed his light aircraft into an office building in Austin, Texas, that housed an Internal Revenue Service (IRS) field office,
killing himself and an IRS manager. Thirteen other people were wounded. His suicide note expressed his anger with the government and the IRS.

**4 March 2010:** John Patrick Bedell, 36, shot and wounded two Pentagon police officers at a security checkpoint at the Pentagon’s metro station, in Arlington, Virginia. With the officers returning fire, the shooter was critically wounded and died a few hours later. The shooter, who had been diagnosed with a bipolar disorder, had expressed strong anti-government extremist libertarian views.

**1 May 2010:** Faisal Shahzad, 30, a Pakistani-American citizen, attempted to detonate a bomb inside a Nissan Pathfinder car in Times Square, New York. After Shahzad fled from the scene, the bomb failed to detonate and its smoke was noticed by a local street vendor, who alerted authorities who succeeded in disarming the bomb. Approximately 53 hours after his attempted bombing, Shahzad was arrested by US Customs and Border Protection (CBP) officers at John F. Kennedy International Airport, after boarding Emirates Flight 202 to Dubai, with his final destination Islamabad, Pakistan. Immediately following the attempted bombing, FBI investigators had quickly discovered his name while checking the identity of the Nissan Pathfinder’s Vehicle Identification Number’s (VIN) ownership, which they had matched to a telephone number Shahzad had provided when he returned to the US States from Pakistan in early February that year. Investigators then were able to sufficiently track his activities to determine that he had purchased an airline ticket for his flight, which enabled them to place his name on a ‘no-fly’ list that ultimately led to his arrest on board the aircraft (just in time for it to be recalled to the gate). After pleading guilty to the 10 counts against him in October 2010, Shahzad was sentenced to life in prison. Although he had undergone training in bomb-making and the use of weapons at a camp run by the Pakistani Taliban in Waziristan, along the Afghan border, he was the sole operative in his operation.

**27 October 2010:** Farooque Ahmed, 34, a Pakistani American from Ashburn, Virginia, was arrested by the FBI for plotting to bomb Washington Metro stations at Arlington cemetery, Pentagon City, Crystal City and Court House. On 11 April 2011, after pleading guilty, he was sentenced to 23 years in prison. Ahmed had told his attack plans to an FBI undercover agent who had informed him that he was an Al-Qaeda operative.

**October and November 2010:** Marine Corps reservist Yonathan Melaku, 22, a naturalized American from Ethiopia and Marine Corps Reserve Lance Corporal, was arrested for carrying out a series of drive-by shootings with a rifle at several military facilities in Northern Virginia. These included the Pentagon, Marine and Coast Guard recruiting offices, and the National Museum of the Marine Corps, in Quantico, Virginia, as well as his attempt to desecrate graves at Arlington National Cemetery. The buildings were unoccupied during the time of the shootings. Upon his arrest, law enforcement agents found bomb making material in his possession. Melaku, who was reportedly self-radicalized into supporting Al-Qaeda, was diagnosed with schizophrenia, and was sentenced to 25 years in prison.

**8 December 2010:** Antonio Martinez (aka Muhammad Hussain), 21, was arrested and indicted for attempting to use an explosive device to remotely bomb a Catonsville, Maryland, Armed Forces recruitment center and kill military personnel. He had packed what he believed to be barrels of explosives into a sport utility vehicle that had been parked by the recruitment center, while under surveillance by the FBI, which, in a sting operation, had foiled the attack by providing him with fake explosives.

**8 January 2011:** Jared Lee Loughner, 22, carried out a mass shooting at an outdoor rally for US Representative Gabrielle Giffords in Tucson, Arizona. He killed six people, and injured 13 others, including Representative Giffords. He was overcome by several persons in the crowd and arrested. In November 2012 he was sentenced to life plus 140 years in federal prison. He
was diagnosed with paranoid schizophrenia, but was also driven by an anti-government rage based on various conspiratorial beliefs promoted by far-right polemicists.48

17 January, 2011: Kevin William Harpham, 36, a lone actor white supremacist, placed a remote-controlled bomb-laden backpack on a bench along the route of a Martin Luther King, Jr. Day parade in Spokane, Washington. The backpack containing the bomb was discovered at around 9:25 am, and defused, with no one injured. The march was attended by 2,000 people. Harpham, who was arrested on 9 March 2011, was sentenced on 20 December of that year to 32 years in prison.

28 July 2011: Nasser Jason Abdo, 21, a US Army Private First Class, was arrested in Killeen, Texas, near Fort Hood; he was AWOL from his army base in Fort Campbell, Kentucky, and was arrested for planning to attack a restaurant frequented by soldiers near the Fort Hood base. Bomb-making materials were found in his motel room, including large amounts of ammunition, weapons and a bomb in a backpack.

28 September 2011: Rezwan Ferdaus, 26, of Ashland, Maryland, was arrested by the FBI for plotting to use a remote-controlled model aircraft packed with C-4 explosives to attack the Pentagon and the US Capitol Building. He was also charged with supporting Al-Qaeda. In November 2012, he was sentenced to a 17-year imprisonment.

December 2011: Abu Khalid Abdul-Latif (AKA Joseph Anthony Davis), 33, and Walli Mujahidh (AKA Frederick Domingue, Jr.), 32, were arrested and indicted for conspiring to use machine guns and grenades to kill military and civilian employees of the Department of Defense’s Military Entrance Processing Stations (MEPS), located in the Federal Center South building in Seattle, Washington. Both had converted to Islam in prison and were radicalized into jihadi extremism. They were sentenced to long-term imprisonment in 2013.

5 August 2012: Wade Michael Page, 40, fatally shot 6 people and wounded 4 others at the “gurdwara” (Sikh temple), in Oak Creed, Wisconsin. After he was shot in the hip by a responding police officer, Page committed suicide by shooting himself in the head. An Army veteran who had trained in psychological warfare, he had been demoted and discharged more than a decade earlier. Following his military service, he played in white supremacist heavy metal bands with names such as Definite Hate and End Apathy.

3 to 12 February 2013: Christopher Jordan Dorner, 33, a Los Angeles police officer, began a series of shooting on 3 February 2013, in Orange County, Los Angeles, and Riverside County, California. Four people were killed and three others were wounded. His shooting rampage ended on 12 February 2013, when he died during a standoff with police responders. His motivation was reportedly seeking vengeance in the form of “unconventional and asymmetric warfare” against the Los Angeles Police Department’s (LAPD) officers and its families for firing him.

15 April 2013: Tamerland Tsarnaev, 26, and his younger brother, Dzhokhar Tsarnaev, 19, detonated two pressure cooker bombs near the finish line of the Boston Marathon, killing three persons and injuring an estimated 264 others. This was followed by subsequent related shootings in nearby Watertown, Massachusetts, on 19 April in which an MIT policeman was killed. With the elder Tsarnaev brother killed in the ensuing gunfight with the police while he and brother Dzhokhar had tried to flee the city, the younger Tsarnaev was wounded and arrested later that evening. He was subsequently convicted and sentenced to death at his trial in Boston in April 2015. Tamerland was considered the primary terrorist operative. Earlier, in March 2011, the Russian Federal Security Service (FSB) reportedly provided the FBI with detailed information that Tamerlan Tsarnaev and his mother Zubeidat Tsarnaeva were “adherents of radical Islam and that he was preparing to travel to Russia to join unspecified “bandit underground groups” in Dagestan and Chechnya.50 While in Dagestan and Chechnya, he may have had contact with adherents of radical Islam, his plot was considered “lone actor” as he and his brother did not receive any direct assistance from a foreign terrorist group. Also, it is reported that Al-Qaeda’s Inspire magazine51 had provided information enabling the
Tsarnaev brothers to build their pressure cooker bombs in Tamerlan’s apartment in Cambridge, Massachusetts, which were “filled with nails, ball bearings and black powder,” with the devices triggered by “kitchen-type” egg timers while reportedly unbeknownst to any of their friends and associates in a position to report such suspicious activities to the appropriate authorities.

14 May 2013: Matthew Ryan Buquet, 37, was arrested in Spokane, Washington, for mailing poisoned letters containing a crude form of ricin to a US District Judge. He was also indicted by a grand jury for mailing a threatening communication to the President of the US and developing, producing, possessing and transferring a biological toxin.

1 November 2013: Paul Anthony Giancia, 23, carried out a shooting rampage with a rifle in Terminal 3 of the Los Angeles International Airport, killing a US government Transportation Security Administration (TSA) officer and wounding seven other people. The shooting spree ended when he was wounded by responding police officers. His motivation was reportedly hatred of TSA and a New World Order conspiracy theory. On 7 November 2016, he was sentenced to life imprisonment without the possibility of parole plus 60 years.

13 April 2014: Frazier Glenn Miller, Jr., 73, of Aurora, Missouri, carried out a pair of shootings at the Jewish Community Center of Greater Kansas City and Village Shalom, a Jewish retirement community, both located in Overland Park, Kansas. Three people were killed, two at the community center and one who was shot at the retirement community. The gunman, originally from North Carolina, a Neo-Nazi activist, was arrested, convicted of murder and other crimes, and sentenced to death.

18 July 2014: Ali Muhammad Brown, 29, was arrested for four terrorism-related killings in Washington State. He had told investigators that the slayings were motivated by his Muslim faith and in revenge against the US for its “evil acts” at home and military intervention in Iraq, Syria, and Afghanistan. Between 2002 and 2004 he had engaged in bank fraud, which prosecutors had charged was in support of the al-Shabaab Somalian terrorist group.

10 April 2015: Mohammed Abdullah Hassan (previously known as John T. Booker), 20, was arrested for plotting to kill American soldiers with what he thought was a 1,000-pound bomb in a van at the Fort Riley military base in Kansas. The fake bomb was provided to him by an FBI informant.

17 June 2015: Dylann Roof, 21, a White Supremacist, shot and killed 9 people, wounding one other person, during a prayer service at the Emanuel African Methodist Episcopal Church in downtown Charleston, South Carolina. He was arrested, after escaping from the scene of the attack.

16 July 2015: Mohammad Youssef Abdulazeez, 24, opened fire at a recruiting station and a naval reserve center in Chattanooga, Tennessee, killing four Marines and a Navy petty officer. He was killed in a shootout with the responding police officers. Abdulazeez was an electrical engineer and martial arts fighter, who had become radicalized into jihadi extremism.

1 October 2015: Chris Harper-Mercer, 26, a student at The Umpqua Community College, near Roseburg, Oregon, carried out a shooting rampage at the college, killing an assistant professor and eight students in a classroom, as well as wounding eight others. After being wounded in a shootout with the responding police, he killed himself. Mercer reportedly had mental health problems and was obsessed with guns and religion and had leanings toward white supremacy.

27 November 2015: Robert Lewis Dear Jr., 57, carried out a mass shooting attack at a Planned Parenthood clinic in Colorado Springs, Colorado. Three people were killed and nine others were wounded. After a standoff that lasted five hours, police SWAT teams crashed armored vehicles into the lobby, forcing the attacker to surrender. The attacker had also placed multiple propane gas tanks near his car, which he may have planned to fire on to trigger an
explosion. An anti-abortion extremist, Dear was found to be delusional and incompetent to stand trial.

2 December 2015: Syed Rizwan Farook, aged 28, and his wife, Tashfeen Malik, 27, conducted a shooting rampage at the husband’s office’s holiday party at the Inland Regional Center, in San Bernardino, California, killing 14 people and injuring 22 others. After fleeing the scene, both were killed in a shootout with police later that day. Farook was employed as an environmental health specialist at the San Bernardino County public health department. Neighbors of the couple, who lived in nearby Redlands, had reported afterwards that they had seen them “acting suspiciously in recent weeks,” working late at night in their house’s garage and receiving numerous packages that appeared out of place. However, they did not report their suspicions “for fear of racial profiling.” The only signs of outward radicalization towards extremism, his co-workers stated, were comments to friends about not wanting to remain in the United States (his parents had hailed from Pakistan) and that upon his return from a visit to Saudi Arabia in July 2014, with Malik, his fiancé, he began growing a long beard (a possible sign of Salafist extremism). In his personal dealings with co-workers, with whom he was not overtly friendly, he had engaged in ideological arguments with a co-worker, who did not regard his views as especially extremist. Nevertheless, it appeared that Farook and Malik had long planned their attack, accumulating a large arsenal of highly lethal firearms and ammunition at their apartment, which they shared with Farook’s mother, who was divorced from her husband, whom she regarded as abusive. It came as a surprise to Farook’s co-workers, therefore, that he and his wife had reportedly maintained a social media relationship with other violent jihadi extremists and that they had posted their allegiance to the Islamic State on the day of their attack.

12 June 2016: Omar Mateen, 29, conducted a shooting rampage at the Pulse Nightclub, in Orlando, Florida, killing 49 persons and wounding 58 others. He was killed in a shootout with the responding police. He had become radicalized into violent Islamist extremism while working at his security company, G4S, where he was employed as a guard for a period of nine years. His radicalization into extremism was known to his co-workers and even the FBI (which did not judge him a security threat), but little was done to remove him from his position as a security guard. In 2013, for example, he was interviewed by the FBI after making inflammatory comments to a co-worker that gave the impression he had possible terrorist ties with Al-Qaeda. In 2014, he again came to the FBI’s attention, when they interviewed him over potential connections with Moner Abu Salh, an American suicide bomber in Syria, who had lived near him in Vero Beach, Florida. Despite these potential red flags, however, his firm still kept him as an employee, although he was transferred to a position that did not require holding a firearm at a kiosk at a gated community in Palm Beach County. In his relations with fellow co-workers, however, Mateen was the subject of several complaints over having “issues and just constant anger” and making frequent homophobic and racist remarks. In another instance of early warning “dots not being connected,” it was reported that in 2007 he was fired by the Florida Department of Corrections after he had threatened to bring a gun to work. This was significant because if it had involved serious misconduct and had it been revealed it would have hindered his future prospects of working for a security company such as G4S. Finally, an ex-wife had accused him of beating her, but this, too, was reportedly not revealed to G4S.

17 to 19 September 2016: Ahmad Khan Rahimi, 28, planted several bombs in the New York metropolitan area, including at a seaside marathon in New Jersey. Three of the bombs exploded and several did not explode. The three bombings wounded 31 people. The bombs included a pipe bomb and a homemade pressure bomb. On 19 September Rahimi was captured following a shootout with the responding police. He was reportedly influenced by Al-Qaeda’s Islamist ideology. In February 2018, he was sentenced to life without parole.

28 November 2016: Abdul Razak Ali Artan, 18, carried out a car ramming and stabbing attack at Ohio State University, in Columbus, Ohio, in which he injured 11 persons. Artan was
a student at the university. The incident ended when a responding police officer shot him dead. That morning he posted a rant on his Facebook page in which he described how he was “at boiling point” and “just couldn’t take it anymore.” He added, “I am sick and tired of seeing my fellow Muslim brothers and sisters being killed and tortured EVERYWHERE. By Allah, I am willing to kill a billion infidels in retribution for a single disabled Muslim.” In the post, Artan also praised American-born Al-Qaeda leader Anwar al-Awlaki, who was killed in a CIA drone strike in 2011 and has been cited as the inspiration for other terror attacks on American soil.

12 August 2017: James Alex Fields Jr., 20, deliberately drove his car into a crowd of people in Charlottesville, Virginia. They were demonstrating peacefully against a protest by a white supremacist rally. One person was killed and 28 were wounded. The driver had espoused Neo-Nazi and white supremacist beliefs. He was arrested for federal hate crime charges, and after being convicted in trial, sentenced to life imprisonment.

31 October 2017: Sayfullo H habibullaevi Saipov, 29, drove his rented pickup truck from Northern New Jersey, proceeded across the George Washington Bridge, and then drove south into lower Manhattan, where he drove for about a mile along a bike path, mowing people along the way, killing eight and wounding 11 others. The vehicle ramming attack ended when he crashed into a school bus. He then jumped out of his wrecked truck brandishing two imitation guns, and shouted, “Allahu Akbar” (Arabic for “God is Greater”) before a New York Police Department (NYPD) officer shot him. In the rental truck, authorities retrieved a handwritten note that, translated into English, said: “ISIS Lives Forever.”

11 December 2017: Akayed Ullah, 27, attempted to detonate an improvised, low-tech, explosive device, which was attached to his body, in a crowded underground corridor of the subway system that connects Times Square to the Port Authority Bus Terminal, in midtown Manhattan, New York. The bomb only partially exploded, injuring the bomber and three bystanders, who sustained minor injuries. The bomber was quickly arrested and hospitalized. It is reported that Ullah began his radicalization into violent extremism in 2014, when he started viewing extremist Islamic State materials on the Internet. He was reportedly influenced by the sermons and writings of Moulana Jasimuddin Rahmani, an extremist Muslim preacher in Bangladesh, who is currently imprisoned for leading a banned group called Ansarullah Bagla Team. It was reported that Ullah had discussed Rahmani’s writings with his wife during his September 2017 visit.

23 March 2018: Hafiz Kazi, 51, an Islamist extremist, drove a KIA minivan through the main gate of Travis Air Force Base, near Fairfield, California. His van was filled with five propane tanks, three plastic one-gallon gas cans, several lighters, three phones and a gym bag with personal items, which were deliberately ignited. With flames inside the van, the vehicle crashed shortly after going through the gate. The driver was fatally burned.

3 October 2018: William Clyde Allen III, 39, a Navy veteran from Utah, was arrested in connection with weaponized letters suspected to contain ricin which were mailed to Defense Secretary James Mattis and Chief of Naval Operations Admiral John Richardson; FBI Director Christopher A. Wray; CIA Director Gina Haspel; and Secretary of the Air Force Heather Wilson. The envelopes containing castor seeds, the base of a deadly toxin, were detected during security screening at a mail processing center on the Pentagon campus. He was reportedly a survivalist who believed that World War III was imminent.

Mid-to-Late October 2018: Cesar Sayoc, Jr., 56, of Aventura, Florida, embarked on a several weeks long mailing of 16 explosive-laden packages against two former presidents, public figures, and media organizations such as CNN. He reportedly had a long criminal history. On 26 October, he was arrested and charged with federal crimes, including interstate transportation of an explosive.

27 October 2018: At around 9:54 am, just as the morning Sabbath service had begun at the Tree of Life synagogue in Squirrel Hill, Pittsburgh, Pennsylvania, Robert Bowers, 54, carried out a shooting rampage, killing 11 and wounding seven others. He used an AR-15 style semi-
automatic rifle and three Glock .357 sig handguns. Bowers, a Neo-Nazi White Supremacist, was apprehended when he gave himself up to the responding police at 10:08 am (after wounding 4 police officers).

**27 April 2019:** John Timothy Earnest, 19, used an AR-15 style rifle to carry out a shooting rampage at a synagogue, in Poway, California, killing one person and wounding three others. Upon fleeing the scene, he called 911 to report the shooting, and was apprehended by a police officer in his car approximately two miles from the synagogue.

**3 August 2019:** Patrick Crusius, 21, carried out a mass shooting attack at a Walmart department store in El Paso, Texas, killing 22 people and wounding 24 others. He was arrested shortly after the shooting and charged with capital murder. A manifesto he had posted on the online message board 8chan shortly before the attack expressed white nationalist and anti-immigrant themes, including citing the Christchurch mosque shootings, as well as a right-wing conspiracy theory known as ‘The Great Replacement’, as motivation for the attack.

**28 August 2019:** William Santino Legan, 19, opened fire with a WASR-10 semi-automatic rifle at the annual Garlic Festival in Gilroy, California, killing three people and wounding 12 others. He bypassed security at the festival’s entrance by cutting through a fence to gain entry. Once inside, he sprayed gunfire on the crowd, but within a minute of firing his first shots, he was shot and killed by three uniformed police officers who were on patrol at the festival. Legan had grown up with his family in the local area. Afterwards, investigators who had searched his house found literature on white supremacy, which may have been the ideological basis for the attack.

**1 November 2019:** Richard Holzer, 27, of Pueblo, Colorado, was arrested by the FBI after he had allegedly accepted what turned out to be phony explosives from undercover agents to bomb the Temple Emanuel synagogue in Pueblo. Holzer’s postings on Facebook had promoted white supremacy and violence, expressing his wish to kill Jews, Hispanics and pedophiles.
The term “lone actor” is used in this chapter. It is recognized that “lone wolf” is a popular usage to characterize what the FBI refers to as “lone offender” attacks. Since the term “lone actor” is also widely used in the literature and encompasses “lone wolf” and “lone offender” type attacks, and is value neutral, it is applied in this article to characterize the type of solo or single offenders examined in the assessment of the threats they present and how to counter them.


FBI Lone Actor Offenders 2019, p. 10.


Rosario, Frank, ‘Tamerlan abuses his future wife, say pals’, New York Post, 24 April 2013, 4:00 am. Available at: https://nypost.com/2013/04/24/tamerlan-abused-his-future-wife-say-pals/.

Gurney, Kyra, ‘Cesar Sayoc was a stripper, a club manager, a dry cleaner and, cops say, a mail bomber’, *The Miami Herald*, 26 October 2018. Available at: https://www.miamiherald.com/news/local/community/broward/article220672300.html.


FBI, Lone Offender 2019, p. 47.


46 Ibid.
47 ADL, Yonatan Melaku. Available at: https://www.adl.org/resources/profiles/yonathan-melaku.
48 Hamm and Spaaij 2017, p. 139.
51 Durante, Thomas. “Investigators discover Boston bombs were detonated by a remote control as suspect admits he learned to build the devices from al Qaeda propaganda magazine,” Daily Mail, 23 April 2013. Available at: http://www.dailymail.co.uk/news/article-2313782/Dzhokhar-Tsarnaev-Boston-Marathon-bomber-admits-learned-build-bomb-Inspire-magazine.html.
60 Ibid.
Bibliography


Web-based Resources


Chapter 22

Prevention of Gun-, Knife-, Bomb- and Arson-based Killings by Single Terrorists

Annelies Pauwels

Lone-actor terrorism is an emerging phenomenon that challenges Western law enforcement agencies. This chapter adds to previous research on the prevention and detection of attacks by single terrorists and does so by focusing on limiting their access to weapons. It analyses the weapons that have been most commonly used by lone offenders in Western Europe over the last twenty years: firearms, knives, explosive and incendiary devices. For each of these weapon types a case study of a recent lone-actor attack is analyzed. The chapter concludes that downstream preventive measures aimed at curbing access to weapons and practical training opportunities can be useful. They can direct lone actor terrorists to more readily available weapons, reducing the lethality of their attacks. The research presents recommendations aimed at further restraining access to weapons and limiting online and on-hands training in the use or manufacturing of weapons. Lone-actor terrorism will most probably continue to exist and possibly rise, as it is a direct response to increasing pressure from law enforcement and is actively promoted by terrorist strategists. While a hundred percent safety from lone-actor attacks is probably unattainable, it is possible to diminish their ability to successfully carry out an attack and limit their lethality.

Keywords: lone-actor terrorism, firearms, knives, arson, improvised explosive devices, European Union
Each new wave of terrorism sees the emergence of lone actors: terrorists that plan, prepare, and commit their acts without direction from a wider organization. Lone-actor terrorism is now re-emerging\(^1\) and its threat is increasing, as their attacks often appear near-spontaneous and aimed at causing large numbers of civilian casualties. This phenomenon poses a challenge to existing law enforcement techniques. The apparent lack of coordination and communication with a wider organization makes it harder to spot the perpetrators through usual surveillance and communication interception. The spontaneity of the attacks complicates efforts to monitor the development of the plot and its disruption. Although lone-actor terrorism seems almost unstoppable, previous research has identified measures that can help prevent lone-actor violence, and detect and disrupt their attacks.\(^2\)

This chapter contributes to that research as it seeks to analyze what can be done to prevent lone-actor terrorists from acquiring their most commonly used weapons. It will do so by examining which weapons were used in lone-actor attacks in Western Europe over the last twenty years. The data presented in this chapter are derived from the Global Terrorism Database (GTD), an open-sourced repository initiated by the University of Maryland. Lone-actor attacks are calculated by the attacks that have been committed by a single perpetrator (variable \(n\text{perp}\)). While the GTD is the most widely used open-source database for calculating the number of lone-actor attacks, it is necessary to also pinpoint its limitations.

First, it is important to note that even when an attack mentioned in the GTD is said to have been perpetrated by a single offender, the perpetrator can have been part of a group. This author filtered out the events that were clearly group-based attacks (i.e., separate attacks occurring on the same day that were part of a larger attack by a group). A clear example hereof is the Brussels attack in March 2016, which is listed in the GTD under two separate entries; one of them by a single perpetrator as the bombing in the Maelbeek metro station was carried out by a single attacker, while the attack at Zaventem airport was registered as a group attack.

Second, data entries in the database only reflect what is known at the moment of inserting the information into the database. This can be altered at a later stage, for instance, when subsequent investigations demonstrate that a single perpetrator had clear links with other individuals or did not act alone.

Third, the GTD contains a large number of unknown perpetrators. Only 17 per cent of the terrorist attacks that took place in Western Europe over the last twenty years have a known number of perpetrators: 279 attacks were committed by a single attacker (\(n\text{perp} = 1\)) and 353 attacks by more than one offender (\(n\text{perp} > 1\)).\(^3\)

Despite these caveats, the “number of perpetrators” (\(n\text{perp}\)) remains a good indicator to examine single offender attacks, as the GTD offers a large enough sample - 279 lone-actor attacks - for analysis. Another interesting variable would be “unaffiliated individual(s)” (\(\text{individual}\)), which indicates that the attack was carried out by one or more individuals not known to be affiliated with a group or organization. Yet, previous research has shown the difficulties in setting boundaries between affiliated and non-affiliated terrorists.\(^4\) For instance, a number of jihadi-inspired attackers claimed to be affiliated to or having pledged allegiance to ISIS, when in reality the connections were minimal or non-existent. On the other hand, right-wing attackers have often been mislabeled as lone actors since the degree to which they were connected with an extreme environment was not fully understood.

It should also be noted that the GTD distinguishes itself from some other data collections by its relatively greater even-handedness. Some previous research on lone-actor terrorism has focused mainly on high-profile attacks (e.g., high lethality attacks) or incidents receiving ample coverage in mass media. This possibly gives a distorted image on the type of weapons mostly used by lone offenders.\(^5\) While GTD is also based on media reports, it strives for objectivity.

Based on the GTD, this chapter presents the main weapons used by lone actors - namely firearms, knives, explosives, and incendiary devices. It will also analyze how lone-actors gained access to and used these weapons, which will be complemented by a specific case study.
The case studies will also cover aspects that provide a better view on the profiles of lone-actor terrorists (e.g., background, behavioral and operational aspects, and the radicalization process).

**Literature Review**

A number of datasets have allowed for empirical, quantitative assessments of lone-actor terrorism in Europe and led to some key findings on which this research builds further. First, there are various types of lone actors. Differences are often related to their ideological background, the degrees of social isolation, alternative pathways to radicalization, pre-attack planning and behavior, and the presence or absence of mental health problems.\(^6\)

Second, despite different profiles, researchers have determined that single terrorists distinguish themselves from group-based terrorists in several ways. In particular, their average age is higher, they are more often confronted with unemployment, despite having a considerable level of education.\(^7\) Ideology, ideas of justice, and empathy would also be more important for single perpetrators than for members of extremist groups or terrorist organizations.\(^8\) Lone actors also suffer more often from mental health disorders than group-based terrorists or members of the general population.\(^9\)

Third, lone offenders are not as isolated as the terminology suggests. Lone actors frequently have interpersonal, political, or operational ties to larger networks. They also often radicalize both in online and offline radical milieus and sometimes receive concrete assistance in the preparation for their attacks.\(^10\)

Fourth, not all lone actors are the “stealthy and highly capable terrorists the ‘lone wolf’ myth alludes to.”\(^11\) They have a lower rate of attack completion and a lower lethality rate when compared to group-based attacks. They also adopt limited operational security measures, and engage in on- and offline ‘leakage behavior’ that provides others with clues about their extremism and their attack plans.\(^12\) However, the lethality of their attacks appears to depend on a number of factors, such as the robustness of counterterrorism efforts, the type of weapon used, and weapon-related training.\(^13\)

This research aims to provide a sense of how the use of weapons by European lone actors has evolved over the last twenty years. Particularly interesting is its focus on cases after 2014, when a significant change in weapon use by lone offenders occurred.

**Lone-Actor Attacks in Western Europe by Weapon Type**

Between 1999 and 2018, Western Europe has witnessed 353 group-based and 279 lone-actor attacks, with a strong increase in attacks by single terrorists particularly since 2011. Whereas between 1999 and 2011, an average of five lone-actor attacks occurred per year, this number increased significantly to the yearly average of 31 in the following years. Lone-actor violence reached a new high level in 2017, when 58 attacks were perpetrated by single offenders. Despite a general increase in terrorist attacks in Western Europe after 2011, the increase of attacks by lone actors is proportionally higher.\(^14\)

Lone actors adhere to various ideologies. However, of the single terrorists operating between 1999 and 2018 whose ideology is known (approx. 65 per cent), most adhere to jihadi (82 attacks) and right-wing (51 attacks) ideologies. Western Europe has also seen a significant amount of separatist (27 attacks) and anarchist (15 attacks) incidents by lone offenders. While separatist attacks have remained rather constant over this twenty-year period, we can see a stark increase in jihadi, right-wing, and anarchist lone-actor attacks since 2011.

Terrorist attacks by lone offenders vary significantly one from another. Many of them are not high-profile attacks and do not lead to high fatalities. One of the main reasons for this disparity is the types of weapons used. The following section will focus on the weapons that
are most often used by European lone actors, highlighting what can be done to prevent access to them and limit their lethality rate.

1. **Firearms**

Firearms are an important weapon for terrorists, including lone actors. Focusing on limiting access to this type of weapon is important for three main reasons. First, firearms cause a higher lethality than other types of weapons. They make up 23 per cent of lone-actor violence in Western Europe since 1999. Since 2011, the proportion of gun-related attacks by single terrorists has decreased, as many of them have exchanged firearms for more readily available weapons. Yet, lone actors that do make use of firearms cause deadlier attacks. Gun-based attacks by lone offenders cause on average 2.3 deaths,\(^{15}\) which is more than most other types of weapons surveyed here. The only exception is vehicle-born attacks, which were on average more than five times as deadly per incident.

Second, the lone actors who did employ firearms, made increasingly use of automatic or semi-automatic rifles. Almost a third of gun-related violence by single terrorists in the last decade has been committed with these types of weapons.

Third, firearms often serve as a facilitating tool to enable attacks through other means. Some of the deadliest attacks that were committed with other types of weapons have been facilitated by the use of guns. For instance, the perpetrators of the vehicle ramming in Nice in July 2016 and the Berlin Christmas attack that same year made use of a gun to obtain their vehicles.
Generally, terrorists access firearms in three ways: they can obtain them from the illicit market, procure them through legal means, or manufacture them. The bulk of firearms used by European terrorists are illegally obtained, most probably due to restrictions in place to buy legal weapons. The dynamics within Europe’s illicit firearms market are largely based on a certain level of trust between the seller and the buyer. Hence, direct or indirect criminal connections are crucial for lone actors to obtain illicit firearms. Many of the current jihadists, including lone actors, have such connections, as a considerable percentage of them have a criminal background. They could thus use their previous criminal networks to obtain access to firearms. Similar criminal connections also are present in extremist groups of other ideologies. Corsican separatists, for instance, maintain social and operational links with organized crime, which facilitates access to illegal weapons.

Lone actors who are not (in)directly connected to any seller of illicit weapons, have more difficulties to get hold of firearms. However, the internet offers them new possibilities since many types of weapons can be bought there. For instance, David Ali Sonboly, who opened fire near a mall in Munich in July 2016, had bought his pistol on the dark web. The internet, thus, serves as an enabler for the trade of illegal weapons that are already on the illicit market; its anonymity increases the safety of both buyers and sellers from prosecution. Nevertheless, acquiring firearms through the internet still bears significant risks for both parties, such as scamming, online detection and monitoring, or the interception of parcels through postal couriers.

Lone actors can also use a legally obtained weapon; however, such cases have so far been exceptionally rare in Europe. European firearms legislation restricts access to this type of weapons for lone actors. This becomes evident in comparison with the US, where access to firearms is less regulated. Guns were used in 38 per cent of attacks by US lone offenders since 2011, making it the main weapon of choice for single terrorists. Most of these shootings involved legally obtained weapons.

Nevertheless, some European lone offenders did use legally obtained firearms in their attacks. One example is Luca Traini, an Italian right-wing extremist who used a legally-owned weapon to target six African migrants in Macerata in 2018. The use of legally-owned firearms by terrorists could become a more stringent problem with the rise of right-wing extremism. The general fascination with weapons in these circles leads to a considerable presence of extremists possessing legal firearms. In 2017, it became known that around 750 right-wing extremists in Germany were in possession of legally acquired guns. Also, the presence of members with a military background in the extreme right-wing movement might increase their legal access to (and knowledge of) weapons.

A third venue for lone actors to obtain firearms is by manufacturing them. This can be done by assembling a weapon from its singular parts, bought either online or offline or manufactured through 3D printing. In October 2019, a German right-wing extremist used homemade firearms, some parts of which were produced with a 3D printer, in his attack on a synagogue and Turkish restaurant in Halle. To date, these cases have been very exceptional, as they require specific knowledge. Yet, 3D printed weapons represent a serious risk since they are very difficult to detect: they do not have a serial number and, being made up almost entirely of plastic materials, they can avoid detection by metal detectors.

The availability of firearms on both the legal and illegal markets is a strong determinant for their use by lone actors. This can also explain the disparity between different countries. The high proportion of legal firearms used by lone actors in the US has already been mentioned above. However, differences can also be found within the EU. For instance, the low level of legal gun ownership in the UK could explain the limited number of lone-actor attacks with firearms in the UK. The type of weapons available is also determinant for the choice of firearms by terrorists. For instance, the availability of semi-automatic and automatic rifles on
France’s illicit market could, in part, explain why the country has seen a relatively high proportion of attacks with such weapons.\textsuperscript{30} While acquiring firearms is one thing, knowing how to use them is another. Generally, European lone actors have had limited firearms training, which could explain why gun-related violence by lone offenders generally does not cause large numbers of victims.\textsuperscript{31} Particular scrutiny is thus necessary for those extremists who have received (para-)military training. Particularly dangerous are European foreign fighters of different ideological currents who fought alongside jihadist, Kurdish, and Christian militias in the Middle East or Ukrainian and pro-Russian militias in the conflict in eastern Ukraine.

The possibilities of obtaining firearms training within Europe can also be limited by introducing and maintaining basic obstacles to practice in shooting ranges (e.g., criminal record checks, registration fees). However, lone actors with a criminal background generally have sufficient opportunities to learn how to handle guns. The following case study on the 2015 attack in Copenhagen shows that such “gangster-terrorists” can carry out deadly attacks.

\textit{Case Study - 2015 Copenhagen Attack}

On 14 February 2015, Omar El-Hussein opened fire at the Krudttonden cultural center in Copenhagen. The target was a public free speech event around a Swedish artist known for his drawings of Prophet Muhammad. Later that evening, the shooter opened fire at a synagogue in the city. The day after he was killed in a shoot-out with the Danish police. The attacker, who had sworn allegiance to ISIS some hours before the first shooting, killed two civilians and wounded five police officers.

The attacker’s criminal connections and skills played a key role in obtaining the weapons used for these attacks, namely an M95 rifle and two old pistols. He had obtained the two pistols through his connections with the gang scene, having been a gang member in his teenage years. He had stolen the rifle from the home of a member of the Home Guard - a volunteer defense organization that supports the Danish military and police. The offender was also familiar with handling weapons as he had been previously sentenced for the possession of an illegal weapon.

The attack also sheds light on how the legal and illegal firearms markets are often interlinked and points to responsibilities carried by legal gun owners. The rifle was a legal firearm, appropriated by the attacker through a targeted robbery. In contrast, the two pistols had entered the illicit market as unregistered weapons, most probably confiscated in an unreported theft.\textsuperscript{32} The legal firearms market thus offers a number of loopholes that can facilitate access to firearms for European terrorists.

The offender’s criminal profile played a key role in his attack. Following a previous conviction for a knife assault on a train, he had spent time in prison, where he seems to have acquired an extremist religious ideology. The fact that he was released from prison just two weeks before the attack highlights the need to focus on reducing recidivism among common and terrorist convicts.\textsuperscript{33} In particular, it is crucial to promote more effective reintegration measures, increase follow-up after release, and improve the exchange of intelligence between prison, law enforcement and intelligence agencies.

The Copenhagen attack seems to undermine the widespread idea of unpredictable and hard-to-prevent lone-actor attacks. The attack was carefully planned and hardly impulsive. The offender had attempted to rent a flat overlooking the Krudttonden cultural center through Airbnb for the preparation of the attacks. The pre-planned nature of the attack is further supported by police reports that the terrorist looked at layouts, photos and Krudttonden’s main website from three different IP addresses prior to the assault.\textsuperscript{34} The attacker also did not act in complete isolation, as four others, all affiliated with criminal gangs in Copenhagen, were arrested for their assisting role. They helped the offender to dispose of the assault rifle after the shooting, provided ammunition for the pistols, and assisted the shooter in the period between
the two attacks.\textsuperscript{35} El-Hussein was in fact not a loner, but firmly embedded in his community, as demonstrated by the large presence of (mainly) youngsters at his funeral.\textsuperscript{36}

\section*{2. Knives}

Conducting a successful attack with firearms can be complicated for lone attackers due to firearms restrictions and the risks of detection while acquiring them. For these reasons, terrorist groups such as Al-Qaeda and ISIS have called on their sympathizers to start a “knife revolution,” as knives are extremely easy to acquire and conceal and can nevertheless be quite lethal.\textsuperscript{37} This type of propaganda has contributed to a stark increase in knife-based attacks by lone actors. While prior to 2011 single terrorists hardly used knives in their attacks, the use of a bladed weapon has increased significantly and, since 2014, has become one of the two primary weapons of choice for lone actors (a position shared with incendiary devices). Stabbings are typically a lone-offender tactic, as group-based attacks with knives remain rare.

Terrorist stabbings generally cause a low level of fatalities, despite the fact that jihadist outlets have provided tips to their sympathizers on how to increase the lethality of knife-based attacks.\textsuperscript{38} Yet, they can cause a high fear effect. Knives are a particularly scary weapon when used by terrorists since they are everyday tools that are readily available. This makes the prevention of the use of knives particularly difficult. Metal detectors can be a useful tool to prevent possible offenders from carrying knives and other sharp objects in crowded places. However, there are loopholes. The three perpetrators at the 2017 London Bridge stabbing, for instance, used 30-cm-long ceramic knives, which could have easily bypassed metal detectors. However, lone offenders do not only use kitchen knives in their attacks: axes, machetes and swords make up a significant percentage of bladed weapons used in lone-actor violence. The following case study illustrates this.

\textit{Case Study: Trollhättan School Attack (2015)}

On 22 October 2015, 21-year-old Anton Lundin Pettersson entered a high school in Trollhättan, Sweden, where he killed three persons and injured one more with a sword. The attacker had never attended this high school himself, but had chosen it as his target because the school was primarily attended by students with an immigrant or foreign background.\textsuperscript{39}

The perpetrator used a Viking sword and carried a Japanese dagger, which he did not use in the assault. He had acquired both weapons online from a legal weapons store in the US shortly before the attack. The weapons, generally sold as collectors’ items, can be easily bought online. Therefore, no alarm bell went off with this purchase, which could have alerted Swedish police or security services. This attack fits the widespread perception of a lone-actor terrorist attack: the offender had a clean criminal record and had not communicated his plan to anyone. However, a closer look at his online behavior could have given a warning. The attacker had been visiting right-wing extremist groups and sites on social media and the internet.\textsuperscript{40} He had also prepared the attack entirely online. In the two weeks prior to the assault, he had consulted online videos on how to use the weapons. In addition, he had bought a black Nazi World War II helmet and a long black coat, which he wore during the attack. He also looked for the other preparatory elements for the attack online: he had studied the route from his home to the school and examined pictures of the building, pupils, and teachers.

The Trollhättan attack is particularly interesting due to the attacker’s mental health condition. Like other lone actors, Pettersson might have suffered from multiple mental disorders, which were, however, never documented. In addition to an autism spectrum disorder, he might possibly also have suffered a gender identity disorder, this being in strong contrast with his worldview and the fact that he idolized and identified with alpha males.\textsuperscript{41} The attacker
could also have been depressed and suicidal, mainly due to his unemployment situation, which he blamed on immigrants. Losing a temporary job shortly before the attack could have been the trigger for the massacre. It is well-documented that mental health issues, such as schizophrenia and delusional disorders, are more often present in lone actors than in group-based attackers or in the general population. However, this should not be used as a pretext to stigmatize mental health patients, as mental health issues alone rarely lead the radicalization process. The overwhelming majority of patients with severe mental health illness do not proceed to violence, and are actually more often victims than perpetrators of violence. Petterson had in his 21-year long life never been diagnosed with a mental disorder. Outreach for suicidal individuals could be useful, as several lone actors have shown a proclivity to commit suicide while taking the lives of others. Here too the attacker appears to have wanted to commit suicide “like a warrior.”

A lone-actor attack that seems hard to predict, the Trollhättan assault demonstrates how measures to increase preparedness against such incidents could help in saving lives. The attack caused a relatively low number of casualties, considering that it took place in a very crowded location at the beginning of a school day. The high level of preparedness of the school personnel turned out to be key in limiting the casualties. A quick reaction of an employee of the school cafeteria, where the attacker had entered the premises, made it possible to notify the police just two minutes later. In addition, the quick warning of the principal to students and staff to lock themselves up in their classrooms most probably prevented further deaths. The CCTV footage of the school premises show the attacker wandering around the school in search for more victims, but mainly finding empty corridors and locked classrooms. It is also evident that the attack would have resulted in more casualties if the perpetrator had managed to gain access to firearms. Petterson had studied mass shootings, such as the Columbine high school shooting and Anders Breivik’s attack. He had also considered joining a shooting club, but abandoned the idea because he could not afford it. Instead, similar to other lone actors before him had done, he made use of a more easily obtainable weapon.

3. Explosives

Explosives are one of the preferred weapons for both terrorist groups and lone actors. Nevertheless, over the last couple of years lone offenders have partially opted for more readily available tools, such as arson. Prior to 2011 explosives were used in 34 per cent of lone-actor attacks in Western Europe; this number decreased to 21 per cent in the following years.

European terrorists surveyed here, mainly used home-made, rather than commercial, explosive devices. Curbing access to explosives is particularly complicated for two main reasons. The know-how on manufacturing explosive charges and devices can be easily found in online and hard-copy instructions. They explain how to construct a wide variety of bombs, including pressure cookers, pipe bombs, and time fuses. Detailed instructions on how to fabricate the explosive charge can be found online relatively easily (but these instructions are not infrequently deficient). European terrorists either used ready-made products (such as commercial explosives, military explosives, or pyrotechnics and propellants) or made their own explosive charges from chemical precursors.

Hard-copy manuals teaching how to manufacture explosives often circulate in radical environments. For instance, Timothy McVeigh learned how to fabricate the bomb that killed 168 and injure 680 people in Oklahoma City from hard-copy manuals on bomb-making. However, the vast majority of bomb-making instructions are available on the internet. For instance, in 2010 Al-Qaeda published in its online magazine Inspire an article titled “Make a Bomb in the Kitchen of Your Mom.” Other downloadable manuals, such as The Anarchist’s Cookbook and The Jolly Roger Cookbook, have provided instructions for the construction and detonation of explosives. There are even YouTube videos providing step-by-step instructions
on how to construct various types of bombs. On any given day there would be almost 300,000 such videos on YouTube, a vast majority of which would be military-type instructional videos.\textsuperscript{50}

Since the material to fabricate explosive charges and devices are commonly used for commercial purposes, it is difficult to curb access to them. Home-made bombs can be made by using common materials, such as switches and battery power sources. A major problem is the availability of chemical precursors used to create home-made charges. For instance, triacetone triperoxide (TATP), an explosive used in various recent terrorist attacks in Europe, can be made from the commonly-available ingredient acetone (found in common household products) and from hydrogen peroxide (which is found in hair bleach and some disinfectants).\textsuperscript{51} Another chemical precursor often used in home-made explosives is ammonium nitrate, which is most commonly found in fertilizers. Anders Breivik used ammonium nitrate to create his vehicle-borne bomb that would greatly damage a government building in Oslo. He created a fictitious agricultural company to acquire large quantities of chemicals and fertilizers and produced explosives without arousing suspicion.\textsuperscript{52}

Breivik’s attack was exceptional, as most contemporary terrorists who perpetrate attacks in the Western world have switched from the use of large explosive charges, carried by vehicle-borne IEDs, to smaller charges and person-borne IEDs.\textsuperscript{53} These are easier to construct and use. The acquisition of smaller quantities of precursor substances also arouses less suspicion and can easily fall below security and regulatory thresholds.\textsuperscript{54} A 2013 EU regulation aims to stop “would-be attackers” misusing certain dual-use materials without curbing access for legitimate bona fide users.\textsuperscript{55} It requires member states to ban non-professionals from acquiring certain chemicals that could also be used in producing explosives. It also obliges businesses which sell or supply such chemicals to report suspicious transactions as well as significant losses and thefts. Yet, some loopholes remain due to a fragmented restriction system among various EU member states. This can make it possible for terrorists to obtain precursor materials in member states with fewer restrictions or lower levels of control.\textsuperscript{56}

Another challenge that remains, is curbing and controlling internet sales. There is often no good method to verify an online purchaser’s identity. In addition, purchasing from various sellers or a combination of retail and internet purchases can avoid raising suspicion. Ahmad Hassan, who in 2017 detonated a TATP-based explosive device on a tube train at Parsons Green in London, had bought the material for his bomb in at least three different venues to avoid suspicion: he got shrapnel from local supermarkets, had hydrogen peroxide delivered to a friend’s address, and bought another ingredient from Amazon.\textsuperscript{57}

Instructions and material for creating explosive devices might be widely available, the myth of the highly lethal Do-It-Yourself (DIY) bomb-maker needs some nuancing. In reality, it remains very complicated to manufacture an effective explosive charge and device based only on online training. The numerous failed explosions with TATP-based explosives, generally perceived as the easiest ones to create, demonstrate this: the Gare Centrale plot in Brussels, the above-mentioned Parsons Green bombing, and the Barcelona plotters.\textsuperscript{58} Lone bombers are also quite often detected during their bomb-making process, due to suspicious injuries or careless handling of the materials.\textsuperscript{59} Furthermore, the lethality of those lone actors that actually manage to reach the point of attack is often low. For terrorist groups, bomb attacks are generally the deadliest type of attacks, with a lethality rate of two deaths per attack, whereas the lethality rate of lone-actor bombings is only 0.9 per attack. Of the 68 bomb-based attacks by European lone offenders over the last twenty years, only seven killed individuals other than the attacker himself.

\textit{Case Study: Attack in Lyon (2019)}

In May 2019, Mohamed Hichem Medjoub left a paper bag containing a parcel bomb in front
of a bakery in a shopping street in Lyon. The jihadi-inspired attack injured 13 persons. With his deed, Medjoub hoped to increase the populist vote in the EU elections two days later, provoking thereby to “push Muslims to revolt.”

The attacker had used a remotely controlled detonator to set off the bomb, which was based on a small quantity of TATP surrounded by bolts and metal airsoft balls as shrapnel. He had manufactured the explosive device and the charge in his kitchen. There, the police found after his arrest three bottles of ammonia, hydrochloric acid and oxygenated water. The perpetrator had studied jihadi-materials and bomb-making videos online and purchased the necessary materials in the months preceding the attack, including through Amazon.

The attacker is one of the few lone actors in this sample who had managed to construct a functioning bomb and set it off remotely. Medjoub’s bomb was effective, yet he had probably hoped to cause a much larger number of casualties from the shrapnel, which is generally used to increase the number of wounded and killed. That not a single individual was killed by his explosion was also due to the small quantity of TATP that was used. Even though the restrictions on chemical precursors most probably deterred him from constructing a deadlier device, the attacker had managed to outsmart restrictions and defy suspicion by ordering the materials from separate places with large time intervals separating the purchases.

However, the attacker was less careful about other aspects of his planning and preparation. Lone actors often adopt limited operational security measures, as they have not or only poorly been trained in this regard. For instance, they may leave virtual traces, give away clues on their intention to strike or expose their radicalism. The attacker in Lyon left such traces. Police reportedly found evidence of contacts with ISIS operatives on his computer. He also left online purchase trails for certain materials he could have acquired more safely in a supermarket, such as the batteries and oxygenated water. He also displayed a lack of attention for his post-attack security, in particular considering his clear intention of surviving the attack (e.g., he used a remotely-controlled detonator, and never claimed the attack). Police were able through video surveillance cameras to retrace his residence, where he had not disposed of incriminating evidence (e.g., the bottles of acid used to manufacture the charge).

4. Arson

Arson attacks have often been used by terrorist groups of different ideologies. Right-wing extremists, for instance, often use fire as a tactic to spread fear among foreigners. In the 1990s, right-wing arson attacks in Germany were aimed at frightening and harming refugees and immigrants. Fire also carries a high symbolic value in the far-right scene, reminding some people of the Nazi period. Arson also plays an important role in many of the American Ku Klux Klan’s ceremonies. Anarchist and left-wing terrorists as well have conducted incendiary attacks against a variety of targets. They often prefer arson over other types of weapons, in part due to the challenges of investigating this type of attack and tracing evidence back to offenders.

More recently, jihadist groups have also encouraged their sympathizers to use arson as a terrorist tactic. Al-Qaeda and ISIS have in their English-language magazines encouraged sympathizers to use arson as a weapon to ignite buildings, forests, and fields. They also provided guidance on various methods of conducting such attacks, and issued a fatwa noting that incendiary warfare is religiously permissible.

In recent years, European lone actors have increasingly made use of arson in their assaults. Between 2014 and 2017, there have been more than eight times as many arson attacks as in the previous 16 years combined. Targets varied from banks to private residences, but most of the recent arson attacks were aimed at places of worship and refugee-related targets. Particularly worrying is how easy it is to conduct such an attack. The materials to start a fire are readily available. Even more advanced incendiary compounds, such as thermite, can be obtained or
manufactured at home. Buying materials to do so, does not always raise the same level of suspicion as purchasing explosive precursors.67

Arson attacks also require limited know-how and are easier to conduct than explosive-based attacks. Terrorists can ignite fires with jerry cans filled with gasoline or by making Molotov cocktails. Jihadist groups recently shared online instructions with their sympathizers and supporters on how to make Improvised Incendiary Devices (IIDs), such as timed or remotely ignited combustibles.68 Detailed instructions on various types of IIDs can also easily be found on open-source websites of other terrorist groups, such as the Animal Liberation Front.69 Such devices can cause major damage, but do not always function properly. In July 2006, two bombs made from gas canisters filled with petrol and diesel, which were placed in suitcases on two trains in Germany, failed to go off when the detonators did not manage to ignite the gas.70 In another case, a firebomb carried inside the perpetrator’s coat into a shop in Belfast in 2013 detonated prematurely, severely injuring the attacker.71

Arson attacks by lone actors have been significantly less deadly than assaults with other weapons. The 63 incendiary attacks that took place in the last 20 years caused only one fatality and seven injuries, other than those injuring the attacker himself. Yet, fire is mainly a tactical weapon. Pyro-terrorism, regardless of the deaths it causes, can be very effective for terrorist groups since it carries a high fear factor. Pyro-attacks are also able to draw large media attention, due to their visual and sometimes symbolic appeal. For this reason, not all arson attacks are aimed at causing casualties. Recent jihadist propaganda has recommended to target parked vehicles and natural resources as well.72 Fire can also aggravate terror attacks that are carried out with other types of weapons, for instance by causing confusion and hindering rescue operations.73

Case Study - Altena Arson Attack (2015)

A substantial number of arson attacks in Western Europe targeted refugees and refugee-related premises. One such attack occurred in October 2015, when two men set fire to a refugee home in Altena, a city in Western Germany. Seven people were in the building at the time of the fire but were alerted by neighbors and managed to escape. The attack caused no casualties, but it generated fear among the direct victims (the residents of the house) and the refugee communities in Germany as a whole.

This attack was highly unsophisticated and committed with the help of readily available materials. The perpetrators had bought the gasoline shortly before the attack at a nearby gas station. Prior to setting fire to the attic of the three-story building (while the residents were sleeping on the ground floor), they had cut the cables of the fire alarm system in the house.74 The unsophisticated tactics and near-spontaneous character of such attacks complicate efforts to disrupt them. It is also challenging to adopt measures preventing terrorists from gaining access to inflammable materials, without curbing the general public’s access to them.

The Altena arson attack highlights the need for broader preventive measures to lone-actor terrorism, in particular curbing online radicalizing material. In the Altena case, the real-life profiles of the two perpetrators showed a strong contrast with their online profiles. They were not already known to law enforcement (one of the attackers was a fireman who had helped to put the fire out again) and had not engaged in violence or extremist activism before. Their radicalism manifested itself exclusively online, as they showed significant activity in right-wing online platforms. Social media echo-chambers can reinforce radical ideas and thus contribute to the radicalization of lone actors. An interesting study conducted two years after the Altena attacks found that towns where per-person Facebook use was higher than average, such as in Altena, experienced significantly more attacks on refugees.75 The internet continues to play an important role in the radicalization process of extremists, including lone actors.76
Therefore the increasing amount of terrorist and propagandizing material online should be met with a more intensive policing of the internet space.\textsuperscript{77}

**Conclusion**

This chapter has illustrated how terrorists make use of the weapons that are readily available. European lone actors, due to current restrictions on traditional weapons such as firearms, increasingly make use of readily available tools, which are often less lethal. This means that a sustained and coordinated pressure for limiting the access to weapons is crucial to preventing and countering the deadliest forms of lone-actor terrorism.

Key to reducing access to weapons is the further harmonization of relevant legislation of EU member states. Gaps in legislation and implementation, in particular with regard to firearms and chemical precursors for explosives, create loopholes that allow terrorists to acquire weapons or the materials to manufacture them. There is also a need to increase restrictions and monitoring of purchases of large bladed weapons, which have become the weapon of choice for European lone actors and can still be freely acquired.

The internet has come to play an increasingly important role in providing terrorists with access to weapons. There is, thus, a need to replicate restrictions that currently exist for on-site purchases also for web shops, such as those selling chemical precursors. In this regard, it is also necessary to enhance the cooperation with, and support of public and private couriers, to facilitate the detection of parcels containing weapons and hazardous material. Cooperation with key third countries is crucial in this, as many weapons are purchased from websites overseas.

Reducing the general availability of weapons can also be useful, in particular for firearms, which are still a widely used and highly lethal weapon. It remains imperative to counter the trafficking of illicit firearms both within the EU and from third countries. New flows of illicit weapons might arrive in particular from conflict areas in the EU’s near neighborhood. Measures should also focus on better registration and monitoring of legally held firearms and impose stricter rules for their storage, as some of these weapons end up on the illegal market.

As terrorists generally use the weapons that are at hand, they will continue to show flexibility and innovation with regard to the weapons they use and how they access them. Therefore, it is necessary to continuously monitor trends in weapon use and update and implement relevant legislations accordingly, including at the EU level.

The lethality of lone-actor attacks is often lower than group-based attacks, partially due to the limited (para-)military training of lone offenders. Therefore, it is crucial to continue imposing obstacles to opportunities to gain weapons training in real life. However, online training has proven to be more important for lone actors. Continued leverage on social media platforms and encryption channels to eliminate and prevent the dissemination of instructional material is therefore necessary. Online monitoring of suspects can be particularly helpful for countering lone-actor terrorism, as they often use the internet for tactical research with limited concern about their operational security.

Nevertheless, lone-actor terrorism is a complex phenomenon. Therefore, a focus on the weapons and know-how should be complemented with a broader preventive focus. The presence of mental health issues and criminal antecedents in a high number of lone-actor profiles also calls for more upstream preventive responses. Actions should include, but not be limited to, improving detection, monitoring and taking care of young people with mental health problems, and rethinking current strategies aimed at reintegrating and rehabilitating those released from prisons.
Annelies Pauwels is a Research Fellow at the Flemish Peace Institute in Brussels, where she focuses on terrorism and violent extremism. Prior to that she conducted research on crime prevention and criminal justice for various international organizations, including the EU Institute for Security Studies (EUISS), the UN Office on Drugs and Crime (UNODC), and the UN Interregional Crime and Justice Research Institute (UNICRI). Her previous research projects have focused on various aspects of international security, including jihadist and far-right terrorism, migration, and organized crime. Annelies Pauwels holds an LLM in International Criminal Law and an MA in Intercultural Mediation, with a specialization in Arabic and Russian. She is fluent in English, French, Italian, and Dutch and has a working knowledge of Spanish, Arabic, and Russian.
Endnotes


3 Between 1999 and 2018, the GTD mentions 3637 terrorist attacks that took place in Western Europe. For 3005 of them the number of perpetrators is unknown \((n_{perp} = 0 \text{ or } -99 \text{ or empty})\), 279 attacks were committed by a single perpetrator \((n_{perp} = 1)\) and 353 attacks were conducted by more than one perpetrator \((n_{perp} > 1)\).


9 De Roy van Zuijdewijn and Bakker, 2016.


14 The average number of lone-actor attacks increased 6.2 times since 2011, whereas the average amount of group-based attacks per year increased 2.3 times over the same period.

15 The Nice attack was not included in these calculations. The perpetrator used a firearm and a vehicle in his attack. However almost all fatalities occurred by the vehicle, rather than with the firearm. The fatalities of this attack are included in the lethality rate of vehicle-borne attacks.

16 Duquet, Nils and Kevin Goris, “Firearms acquisition by terrorists in Europe. Research findings and policy recommendations of Project SAFTE,” Flemish Peace Institute, Brussels, 2018, p. 120.


34 McPherson, Ross, “New information indicates 2015 Copenhagen terrorist attacks were pre-planned,” The Copenhagen Post Online, 19 October 2018. Available at: http://cphpost.dk/news/new-information-indicates-2015-copenhagen-terrorist-attacks-were-pre-planned.html.
36 “Copenhagen gunman’s burial attracts hundreds,” The Local. Available at: https://www.thelocal.dk/20150220/copenhagen-gunman-funeral-attended-hundreds.
38 Ibid.
40 The Local, “Killer spent two weeks planning school attack,” 8 March, 2016. Available at: https://www.thelocal.se/20160308/killer-spent-two-weeks-planning-school-attack.
41 Erlandsson and Meloy 2018.
43 Ibid.
45 Erlandsson, Åsa and J. Reid Meloy 2018.
46 Ibid.

56 Ibid.
59 Ellis et al., 2016, p. 9.
64 Koehler 2016, p. 107.
67 Ibid.
68 National Counterterrorism Centre, Recognizing Arson With a Nexus to Terrorism, Joint CT Assessment Team, First Responder Toolbox, April 2017. Available at: https://www.dni.gov/files/NCTC/documents/jct/firstrespondertoolbox/First_Responders_Toolbox-Recognizing_Arsan_With_a_Nexus_to_Terrorism_Originally_Published-14_April_20171_May_2019-survey.pdf
72 National Counterterrorism Centre 2017.
74 Deutsche Welle, “German fireman admits in court to setting fire to refugee house,” 31 May 2016. Available at: https://www.dw.com/en/german-fireman-admits-in-court-to-setting-fire-to-refugee-house/a-19296140


Bibliography


McPherson, Ross, “New information indicates 2015 Copenhagen terrorist attacks were pre-planned,” *The Copenhagen Post Online*, 19 October 2018. Available at: http://cphpost.dk/news/new-information-indicates-2015-copenhagen-terrorist-attacks-were-pre-planned.html


The Local, “Killer spent two weeks planning school attack,” 8 March, 2016. Available at: https://www.thelocal.se/20160308/killer-spent-two-weeks-planning-school-attack.


Web-based Resources


In recent times, a significant amount of policy development has been directed towards assessing, countering, and mitigating the threat from improvised explosive devices (IED) in urban environments. Much of this has been in direct response to the impact of specific terrorist attacks that have occurred in recent times in many cities. Less attention has been positioned towards understanding how policy- and practice-based approaches in disciplines that are not considered mainstream in the counterterrorism discourse could be used to enhance the resilience of new developments linked to the protection of crowded places. This chapter seeks to overcome this by critically analyzing the fundamental questions of “what measures have been undertaken” and, to a lesser extent, “who should be responsible for counterterrorism-related protective security measures?”

Keywords: bombings, IEDs, VBIEDs, protective security measures, target hardening, situational crime prevention, terrorism.
Although, terrorism has been called “the philosophy of the bomb,” in recent years only about half of all terrorist attacks involve high-explosives or homemade bombs. As access to powerful explosives has been made more difficult by governments, there has been a shift to self-fabricated bombs. The use of such improvised explosive devices (IEDs) by terrorists including vehicle borne IEDs (VBIEDs) is a frequent tactic in terrorist campaigns. Such attacks not only result in fatalities and injuries to those caught up in the explosion, but they also damage physical structures and have the potential to bring down buildings. Additionally, as Meyer notes, the resulting “media coverage of bombings is considerably more graphic than coverage of, say, a shooting.” Of the twenty most fatal terrorist attacks recorded in the Global Terrorism Index for 2018, nine involved the use of explosives, with eight of these undertaken by suicide bombers including three VBIEDs. The remaining attacks saw explosives detonated during the Taliban’s assault on the major city of Ghazni, Afghanistan. The focus of this chapter is on the prevention of bombing attacks by terrorists. Drawing upon a diverse body of literature, it discusses the various measures which can be undertaken to prevent such attacks and considers who is responsible for preventive measures. To assist in our understanding of protective security measures, we first consider some of the theoretical considerations behind them.

Rational Choice Theory and Situational Crime Prevention

Much of the literature is informed by rational choice theory, which aims to explain human behavior and “assumes that people, whenever faced with several possible options, choose the one they expect to have the best overall outcome.” Rational choice theory has been further used by criminologists with respect to decision-making by criminals. It considers criminal behavior “as the outcome of decisions and choices made by the offender.” Consequently, if the benefits outweigh the costs, the potential offender will commit the crime. Crucially, rational choice theory has informed situational crime prevention (SCP), which attempts to reduce specific crimes by affecting the situational determinants (e.g., the immediate environment and opportunity reduction) of that crime and thereby making it less likely to occur. Thus, SCP is concerned not with why a crime occurs but with how a crime is committed. As such, it belongs to what Clarke terms a “family” of similar preventative approaches found within environmental criminology including Crime Prevention Through Environmental Design (CPTED) and by creating a “defensible space.” CPTED involves crime control through the design of the physical environment and the implantation of social policies that reduce the rewards of criminal behavior while also increasing the risk involved in committing a crime.

The concept of “defensible space,” put forward by Newman, focuses on the manipulation of the built environment to reduce opportunities for crime. It emphasizes four key areas: territoriality (i.e. increasing residents sense of ownership of space), surveillance (i.e. increasing opportunities for natural surveillance), image (i.e. overall look and characteristic of a place that will give either a positive or negative impression), and milieu (i.e. making the most of a development’s location to places that will help to prevent crime). For scholars like Clarke, crime is always a choice and therefore “creating unfavorable circumstances is the objective of situational crime prevention.” Subsequently, SCP involves five main mechanisms by which to affect the potential offender’s decision-making process, namely:

1. increasing the effort (e.g., target harden, control access to facilities, screen exits, deflect offenders, and control tools/weapons);
2. increasing the risk (e.g., extend guardianship, assist natural surveillance, reduce anonymity, utilize place managers, and strengthen formal surveillance);
3. reducing the rewards (e.g., conceal targets, remove targets, identify property, disrupt markets, and deny benefits);
4. reducing the provocations (e.g., reduce frustrations and stress, avoid disputes, reduce emotional arousal, neutralize peer pressure, and discourage imitation); and

5. removing excuses (e.g., set rules, post instructions, alert conscience, assist compliance, and control drugs and alcohol).\textsuperscript{10}

Before looking at the use of SCP measures to counter terrorism and, more specifically, preventing bombing attacks by terrorists, it would be remiss of us not to acknowledge that SCP is not without its critics. A major criticism of SCP is that it does not solve the problem of crime, but merely displaces it from one place to another.\textsuperscript{11} A number of different types of displacement have been identified, namely:

- temporal (i.e., committing the intended crime at a different time);
- spatial (i.e., committing the intended crime at a different location);
- target (i.e., changing the target of the crime to another object);
- tactical (i.e., committing the intended crime using a different method); and
- functional (i.e., committing a different type of crime from the originally intended crime).\textsuperscript{12}

Research has shown that displacement had occurred as a result of SCP measures, for example following the introduction of steering column locks in new cars in the UK in the 1960s, vehicle theft was displaced to older models. In New York City, a police crackdown on subway crime displaced robberies to the street.\textsuperscript{13} Other research has found that SCP measures did not result in displacement, for example, the use of passenger screening and boarding gate security searches in the US dramatically reduced criminally motivated hijackings.\textsuperscript{14} Reppetto, in his study of robbers and burglars, concluded that “some crimes are so opportunistic that their prevention in one circumstance will not lead to their occurrence in another. Even in instances where offenders blocked in one sphere would wish to operate in another, limits and costs will lessen the frequency of operation.”\textsuperscript{15} Interestingly, researchers have found that the introduction of SCP measures may result not in displacement, but in positive benefits in terms of general crime reduction beyond the immediate focus of the measures introduced, known as the “diffusion of benefits.”\textsuperscript{16} For example, the installation of live CCTV cameras (two real cameras and three dummy ones) to combat vandalism and graffiti on a fleet of 80 double-deck buses in the North of England saw a sharp reduction in vandalism and graffiti across the entire fleet while the introduction of electronic tagging of library books at the University of Wisconsin to combat book thefts saw a decline in thefts of other material such as videocassettes.\textsuperscript{17} Other criticisms of SCP relate to the theoretical and conceptual adequacy of the approach (e.g. it ignores the root causes of crime and is a-theoretical), and the social and ethical issues that situational interventions raise (e.g. it promotes a “fortress society” and encourages Big Brother surveillance).\textsuperscript{18}

Despite these criticisms, proponents of SCP argue that mechanisms should be focused on specific crimes such as burglary rather than on a broad category of crime such as theft as “the situational determinants of any specific category of crime are quite different from those of another one, even one that seems similar.”\textsuperscript{19} To this end, Clarke and Newman identified four key pillars of situational opportunities that terrorists exploit in order to engage in terrorism, namely targets, weapons, tools, and facilitating conditions.\textsuperscript{20} Targets concerns the physical structures where terrorist attacks take place - these can be either static (e.g. monuments and transportation hubs) or moving (e.g. vehicles and planes). Weapons refers to the means utilized by terrorists in their attack on the target (e.g., explosives, guns, and knives). Tools involve the everyday objects used to carry out their attacks (e.g., money, identification cards, and vehicles). Facilitating conditions include those factors that permit the terrorist attack to occur (e.g., access to buildings and lack of identification requirements). Using established SCP techniques, they developed a terrorism risk assessment template for evaluating the desirability of targets to terrorists, based on eight criteria, known by the acronym EVIL DONE (exposed, vital, iconic,
legitimate, destructible, occupied, near, and easy). Exposed targets are those that stand out and attract attention (e.g., a high-rise building). Vital targets are necessary to the survival of people in their daily life (e.g., water supplies and power plants). Iconic targets are symbolically significant to society (e.g., the White House and the Statue of Liberty in the US). Legitimate targets are deemed deserving of an attack (e.g., military personnel or government buildings). Destructible targets are those that are easily destroyed in comparison to other targets. Occupied targets are those with more potential victims. Near targets are those that are relatively close in proximity to where the terrorists are based. And, finally, easy targets are those easily accessed or with little or no security measures in place. Clarke and Newman argued that we “must identify vulnerable targets, prioritize them for protection, analyze their specific weaknesses, and provide them with protection appropriate to their risks.”

Using Clarke and Newman’s EVIL DONE terrorism risk assessment template, Boba produced sets of items for each of the eight EVIL DONE criteria. In doing so, she created a methodology involving ordinal-level indexes (where five is the highest score and signifies the value showing the most vulnerability and zero is the lowest score for each of the criteria) that could be used by practitioners to score consistently across potential targets. To illustrate, within the exposed criteria, large high-rise structures in an urban area (e.g., the Washington Monument) would rank as a five in Boba’s index, while a cluster of buildings in an urban area (e.g., a university campus) would rank as a one, namely a low exposed status. While Boba’s work provided a system for individual target assessment of terrorism risk, it did not apply the methodology to assess the attractiveness and vulnerability of actual targets selected by terrorists.

In contrast, Ekici et al. employed the EVIL DONE approach to terrorist targets (actual and potential) in Istanbul, Turkey in the period 1990 to 2006, by looking at the three major terrorist groups operating in the country. These were the Kurdistan Workers’ Party (PKK/KONGRA-GEL), the Revolutionary People’s Liberation Party-Front (DHKP/C), and Turkish Hezbollah. Their study involved tasking Istanbul-based intelligence service officers from the Turkish National Police with rating identified targets from the perspective of each of the three respective terrorist groups. They found that the attractiveness of targets was similar across the three terrorist groups. Adding to this small but growing body of literature concerning SCP and terrorism, Gruenewald et al. used data from the American Terrorism Study to assess the attractiveness and vulnerability of targets selected by environmental and animal rights extremists or eco-terrorists between 1987 and 2012. Their study operationalized the eight criteria of the EVIL DONE framework into applicable measures of eco-terrorism targets with eight corresponding hypotheses. They found that eco-terrorists had a preference to attack targets where access was not restricted and where the general public rarely frequented either during the day or at night. Additionally, eco-terrorists selected “easy” targets that were not protected by security measures. They also suggest “that eco-terrorists most commonly attacked or planned to attack legitimate targets, or those targets most directly responsible for engaging in behaviors viewed as harmful to animals and the environment.”

Other research has examined particular SCP measures and concluded that increasing the effort and risk through target hardening can lead to unintended consequences, not only in terms of displacement but also with regard to transference. Enders and Sandler found that following the introduction of measures to increase the security at American embassies (e.g. perimeter defenses, physical security, and the screening of visitors) in the 1980s, attacks shifted from embassy grounds to diplomatic officials outside of their secure compounds. They also discovered an increase in kidnappings and assassinations following the installation of metal detectors at airports. As Morris noted, such a finding “does not necessarily suggest that we should abandon target-hardening efforts.”

Indeed, more recent research has suggested that displacement is not inevitable. Perry et al. have evaluated the effectiveness of the Israeli West Bank Barrier to prevent suicide bombing
attacks, finding that the Barrier “together with associated security activities was effective in preventing suicide bombing and other attacks and fatalities with little, if any, apparent displacement.” Hsu and McDowall’s study considered whether target hardening of the aviation sector and American embassies and diplomats resulted in more lethal terrorist attacks against those targets between 1970 and 2001 using time-series data from the Global Terrorism Database. They concluded that the protective security measures undertaken, did not systematically increase casualty incidents for the protected targets. Moreover they “suggest that perhaps attacks against hardened targets are more prominently based on symbolism rather than violence.” A similar finding was discovered by Hasting and Chan in their examination of the relationship between target hardening and the value that a terrorist group derives from the attack, using a case study of aviation security. Thus, even though a target has been hardened, it now has more symbolic value to the terrorist group concerned and “regardless of whether there are any casualties, attacks on fortified targets signal strength and determination that underscores the credentials of the terrorists.”

With the theoretical considerations behind SCP discussed, we can now turn our attention to the practical steps that can be taken to prevent bombing attacks by terrorists.

Target Hardening and Strengthening

Target hardening measures are “meant to either make it impossible to attack the target or to have an attack on a target judged not worthwhile by terrorists, given the elevated risk, effort, or difficulty associated with a successful strike.” In contrast, strengthening measures are those undertaken to increase the overall stability and strength of a structure. With respect to bomb attacks, Meyer identifies four main strategies for reducing the expected harm from bomb explosions, specifically: “reducing the probability of the attack being successful; reducing the damage from an explosive attack; reducing the offender’s benefit from a successful attack; and increasing the offender’s cost of attacking.” Such strategies are in keeping with the core tenets of SCP, namely increasing the effort and risk while reducing the rewards. Much of the protective security literature emphasizes the importance of a layered approach to security and “describes the practice of securing a site by applying multiple layers of complementary protective security measures.” A layered approach involves four independent security layers, namely deter, prevent, protect, and contain - with each layer representing an integrated system of measures or controls designed to either stop a terrorist attack from occurring or to mitigate it consequences if it does. Deter and prevent are aimed at reducing the likelihood of a terrorist attack while protect and contain are intended to reduce the attack’s impact. Thus “if implemented correctly, layered security ensures that the failure of any single layer – which may consist of different security measures – will not significantly compromise the overall security of the place being protected.”

In order to reduce the probability of a bomb attack being successful, a number of measures can be taken both to deter and prevent bombings. Two main types of bombs can be identified, namely mailed bombs and placed bombs. Placed bombs comprise person-borne IEDs and VBIEDs and include suicide bombers. As Atlas and DiGregorio noted: “the majority of bombs are placed so that controlling access is the most important thing that facility managers can do to protect their facilities.” Establishing a secure perimeter with access control procedures can guard against terrorists gaining access to a site while allowing authorized personnel entrance. Utilizing comprehensive screening procedures can prevent devices from entering a potential target’s space. For example, for a person-borne IED (placed bomb), either a hand-carried device or suicide bombers vest, screening stations at entrances, the requirement that visitors show identification to reception personnel for admittance to a building, the keeping of detailed logs recording visitor and service staff arrival and departures times, and the use of easily distinguishable identification badges for staff and visitors, can prevent such devices from
reaching their intended blast location. Bomb sniffer dogs and portable explosive detection units can also be employed. For example, K-9 (police dog) teams and explosive trace detection devices that scan the air for traces of bomb materials are already deployed at Pennsylvania Station in New York.\textsuperscript{45} For air travelers, a host of measures have been introduced post-9/11, including the use of behavioral detection officers, air marshals, x-rays and hand checks for baggage (both checked in and carry on), explosive trace detection, pat-downs, the use of full body scanners, and limitations on the amount of liquids carried in hand baggage.\textsuperscript{46} In terms of a device sent through the post (mail bomb) screening in mail rooms is required and the location of the mail room should be placed on the exterior of a building with consideration given to blow out walls in the event of a letter bomb detonating.\textsuperscript{47}

For devices involving vehicles, vehicle access control is important. This includes separation of access points by vehicle type (e.g., employee, service, or visitors’ vehicles), underground parking and public parking close to the site must be secured or should be non-existent while street parking adjacent to the potential target should not be permitted.\textsuperscript{48} Additional measures can include controlling the flow of traffic around targets located in urban areas. This can be done through road closures, speed limits, traffic redirection and the use of high curbs, median strips, and bollards.\textsuperscript{49} As Young noted: “the principal reason why this attack vector is popular as a weapon of terrorism is the ability to deliver relatively large, concealed payloads in proximity to the target.”\textsuperscript{50} VBIEDs can involve moving cars or trucks (e.g., in suicide attacks) as well as stationary vehicles (e.g., bomb detonates in a car on timed delay or by remote signal). For both types, increasing the separation distance between the vehicle and the target, the stand-off distance, is crucial. By increasing this distance, the terrorist is required to increase the payload to achieve the desired objective. For example, an increase in stand-off distance from 10 to 20 feet would need a corresponding increase in payload from 100 to 1,000 lb of TNT-equivalent explosive to achieve a total building destruction and would mean moving from the use of a car to a truck.\textsuperscript{51} Thus, increasing the stand-off distance is viewed by many as the most effective defense against a VBIED.\textsuperscript{52} Therefore, physical barriers are required to counter the threat of VBIEDs. For a stationary vehicle bomb, the barrier need only to make it difficult to cross the boundary without being noticed, whereas for a moving VBIED the barrier must be capable of stopping the vehicle, thereby providing a hard stop to the terrorist attack.\textsuperscript{53} Such vehicle security barriers can include passive mechanisms like static bollards, strengthened planters and street furniture (e.g. seating, bike racks, and lighting), walls, fences, and topographical features like water, berms, bunds, and ditches. They can also involve active measures including retractable blockers, bollards, and gates.\textsuperscript{54}

Measures designed to increase both natural and mechanical surveillance opportunities can also reduce the probability of a bomb attack being successful in that a placed bomb may become more visible.\textsuperscript{55} Natural opportunities can take “informal” and “low tech” forms such as good lines of sight, the absence or removal of blind spots and hiding places, consideration of the placement of windows and the replacing of litter bins with clear plastic bags.\textsuperscript{56} Examples of mechanical surveillance opportunities include the installation of CCTV, including “second generation CCTV,” where “cameras actively identify and inform operators of phenomena worthy of attention rather than passively receive events,” automatic number plate recognition (ANPR), intelligent pedestrian surveillance, and facial recognition technology.\textsuperscript{57}

In terms of mitigating the damage or impact from a bomb attack and thereby reducing the terrorist’s expected benefit, a range of options are available and involve the protect and contain layers. For suicide bomb attacks involving VBIEDs, preventing vehicle approach to the target is required. Here measures can include increasing stand-off by installing physical obstacles such as barriers and bollards, and traffic calming measures such as chicanes and bends, which force vehicles to slow their speed or risk flipping over.\textsuperscript{58}

Blast resistant construction - once the domain of military facilities and critical infrastructure assets - is increasingly being considered for commercial developments and
buildings. As already noted, stand-off distance is considered the most effective measure against a terrorist bomb, especially a VBIED. However, if distancing is not present or cannot be imposed, then other measures exist to protect or reduce a bomb’s damage. Many blast resistance measures are aimed at preventing progressive structural collapse by increasing the structure’s ductility and involve incorporating more columns or load carrying walls and the strengthening of upper floor systems. Progressive structural collapse is defined as “the spread of local damage, from an initiating event, from element to element resulting, eventually, in the collapse of an entire structure or a disproportionately large part of it.” One example where progressive structural collapse was evident following a terrorist attack is the Oklahoma City Bombing in 1995, which saw a stationary VBIED (box truck) containing the equivalent of 4,000lb of TNT detonate just 16 feet from the north side of the Alfred P. Murrah Federal Building. Another example is the 1983 attack on US marines at their headquarters at Beirut International Airport in Lebanon. This attack involved a moving VBIED (stakebed truck) loaded with the equivalent of over 12,000lb, which breached the perimeter of the compound and was driven into the building where it exploded. As Eytan noted: “much has been done recently to devise and implement protective hardening measures in new structures…. much less has been done to strengthen existing structures, as this is considerably more difficult and more expensive, if at all feasible.” In existing structures and buildings, retrofit measures can be undertaken to prevent progressive structural collapse, e.g. by strengthening columns on lower floors. Measures include adding concrete around the columns, the reinforcement of existing columns with steel plates or the strengthening of column connections to the adjacent structural elements. The dislocation of slabs by the blast can be countered by the strengthening of existing slabs for uplift loads with extra steel (plates or meshes), concrete layers or sheets, connections between the slabs and supporting walls. Beams can also be reinforced by additional steel shielding slabs.

Facade protection can help to prevent or mitigate blast injuries and would include laminated glass, blast resistant curtain wall protection, “stand-alone” or punched windows incorporated into the facade of a building and bomb blast net curtains designed to catch and contain projectiles and shrapnel from the blast. Injuries or deaths arising from shards of broken glass are common following an explosion. Retrofit measures to prevent injuries from glass range from adding blast curtains, the application of anti-shatter films to existing glazing, the introduction of inner “catching” systems utilizing energy absorbing strong plastic or steel cables, bars or strips and the replacement of existing glazing with blast resistant glazing. For new buildings, there is the option of using blast and fire resistant materials such as laminated glass, which crumbles rather than shatters and reinforced concrete. Retrofit measures to mitigate injuries from masonry wall debris include the addition of layers of plastic or sheets to the inner side of walls, the addition of extra shielding blast walls (e.g. reinforced concrete and the use of layered configurations like steel-concrete-steel), and the replacement of extant masonry walls with blast resistant walls.

Providing good evacuation routes including good signage, safe refuge areas, and emergency lighting has the potential to reduce the impact of a bomb and in doing so reduce both the terrorist’s benefit and rewards from undertaking the attack. For example, following the 1993 bombing of the World Trade Center, a number of improvements were made to facilitate the safe evacuation of the buildings’ occupants, including the improvement of the voice communication system on each floor. In addition, evacuation drills were held bi-annually with staff training and personal evacuation chairs provided for disabled employees. Furthermore, in the stairwells of each tower, photoluminescent paint was used to mark the steps and handrail, and also to illuminate travel paths. Additional, photoluminescent signs were posted on the stairwell’s doors specifying the stairwell name, floor level and the closest re-entry floors. A backup power supply was added for emergency systems while battery packs were added to the emergency lights in the stairwells. As Proulx and Fahy noted: “the
improvements made to the buildings, the training received, the behavior of the occupants, all contributed to allow nearly all of the occupants present below the impact points to escape on September 11th.\textsuperscript{71}

For terrorists not engaging in suicide attacks, a number of measures aimed at increasing the offender’s cost of undertaking a bomb attack center around the risk of being apprehended by security personnel and law enforcement. Such measures include foot and vehicle patrols by security personnel, intrusion detection systems, blast resistant CCTV, with surveillance footage located on external servers, and extensive CCTV coverage in potential target areas so that if some cameras are destroyed in the blast, others may have captured images of the assailant.\textsuperscript{72} However, as Shafoe et al. noted regarding suicide bombers: “the potential deterrence of arrest and punishment becomes meaningless and the traditional need to have a means of escape after the act becomes unnecessary.”\textsuperscript{73}

The use of a variety of SCP measures has at times resulted in the creation of security zones around whole city sections - most notably in Baghdad, Belfast, London, New York, and Washington. Baghdad’s Green Zone (also known as the International Zone) encompassed a heavily fortified seven square mile district housing the American, British and other coalition embassies, and the Iraqi National Assembly Building, which saw roads and neighborhoods sealed off, a limited number of entrances guarded by military checkpoints, and some 12,000 blast resistant reinforced concrete T-walls, measuring 12 feet high, and weighing 14,000lb used to line streets and block off intersections.\textsuperscript{74} In response to the threat posed by Irish Republican terrorism over the course of some 30 years, both Belfast and London have witnessed the militarization of its urban space and parts of both cities were characterized by “fortress architecture.”\textsuperscript{75} Between 1970 and 1975, Belfast experienced a deteriorating security situation with some 1800 explosions, Bloody Friday (21st July 1972), alone saw 19 bombs (15 VBIEDs and 4 person-borne IEDs) detonated in less than an hour across the city.\textsuperscript{76} In an effort to combat the Provisional IRA’s use of stationary VBIEDs, unattended parking was banned in the city center from March 1972. In July 1972, temporary barbed wire and concrete barriers were placed at entrances to the small shopping streets of the city center while pedestrians and delivery vehicles were stopped and searched by security forces.\textsuperscript{77} By 1974, the barbed wire and concrete had been replaced by more permanent iron and steel barriers, and with the merging of four of the seven existing security areas, a single extensive security zone was created, which encircled the city’s main shopping streets. Entrances were either sealed off or staffed by security personnel - Belfast’s “ring of steel” was complete. As Brown noted: “since the creation of the security zone there has been a marked decline in the number of terrorist attacks on central Belfast and a concomitant increase in levels of trade and private sector investment.”\textsuperscript{78}

In 1992, London enacted its own “Ring of Steel” in the City of London and a “mini ring of steel” known as an “iron collar” in London Docklands in 1996 following bomb attacks by the Provisional IRA.\textsuperscript{79} A territorial approach involving security cordons covered both areas with the number of entrances reduced and then secured. Use was made of roving and static police checkpoints, no parking areas and sophisticated technology including CCTV and ANPR.\textsuperscript{80} As Coaffee pointed out: “since the ring of steel’s implementation there have, to date, been no further bombs in the City, and a number of other benefits have emerged, such as a reduction in recorded crime, pollution and traffic accidents.”\textsuperscript{81} In New York and Washington, especially in the aftermath of both the Oklahoma Bombing and 9/11, Jersey barriers made out of three feet high and ten feet long concrete blocks sprung up around monuments. There were new visitors screening stations (e.g., at the Washington Monument) and chain link fences. In addition, roads were closed off (e.g., closure of Pennsylvania Avenue between 15th and 17th Street immediately north of the White House) and bollards and bunkers were dotted around both Washington DC and New York.\textsuperscript{82}
Within the literature on damage limitation, a number of scholars contend that protective security measures designed to counter terrorism including bomb attacks have negative impacts on the urban environment. Matijosaitiene and Petriashvili noted that “antiterrorism design often creates a hostile environment for daily users by scarring downtowns with desolate security zones, repetitive rows of bollards, and threatening architecture.”

While scholars like Benton-Short, Jasiński, and Graham have suggested that such measures result in the militarization of cities, the securitizing of everyday spaces, a “hardening” of urban landscape, restricted access to public space and facilities by residents, and constant control and 24/7 surveillance through state-of-the-art technologies. Others suggest that visible counter terrorism measures in urban spaces are fear-inducing and result in undue anxiety among the public. They claim that counter-terrorist measures act as a continual reminder to the user or visitor that the area is considered a potential terrorist target. However, Dalgaard-Nielsen et al.’s research - conducted in Denmark - suggests otherwise. They found that far from having negative effects upon residents, “visible security measures apparently made people feel safer.”

Thus, the empirical evidence to date has been somewhat limited in this area and the results rather contradictory

Whilst overt protective security measures are still evident, there has been a shift towards more “toned down” security with invisible and sensitive measures. This shift emphasizes that security interventions should be acceptable to the public, aesthetically pleasing, and less obtrusive. Thus, as Coaffee et al. noted: “security features are being increasingly ‘camouflaged’ – or covertly embedded within the urban landscape. These counter-terrorism features may be ‘invisible’ to the unaccustomed eye and do not obviously serve a counter terrorism purpose. They include aesthetically landscaped barriers or street furniture and collapsible pavements.” The American embassy in London is emblematic of this shift. In the aftermath of 9/11, the embassy based in Grosvenor Square had become increasingly fortified with a perimeter of high fences, concrete blocks, and bollards, while armed guards were stationed outside the site and one side of the square had been closed to vehicle access. In 2009, the American government announced a design competition for a new embassy to be built on the south bank of the River Thames in Nine Elms. The new embassy opened to the public in December 2017, and was inspired by European castle architecture, involving a highly protected structure surrounded by moats and ditches. The embassy is a 200-foot (11-storey blast proof) glass cube, which sits on a hill, thereby maximizing visibility. It has a “seclusion zone” of 100 feet from the nearest street, is surrounded by a reflecting pool and is built within a self-contained site of 4.5 acres mainly planted with trees and grasses. The multi-level site acts as a defensive buffer zone in which the architects have minimized the use of fences and walls by utilizing “tactical topography of ‘hostile vehicle mitigation’ techniques woven into an undulating idyll of prairie grasses and weeping willows.”

With some practical ways that exist to prevent bombing attacks by terrorists discussed, we can now turn our attention to the issue of who ought to be responsible for protective security.

Responsibility for Protective Security

Protective security standards with respect to American government and military facilities at home and abroad were developed and introduced in the wake of deadly terrorist attacks, primarily those involving VBIEDs. The April 1983 terrorist attack on the American embassy in Beirut, Lebanon, saw a suicide bomber crash a truck into the front of the building and detonate approximately 2,000 lbs. of explosives. It resulted in a review of security at American overseas facilities and led to the development of the so-called Inman standards for embassy planning. These included standards requiring minimum setbacks of 100 feet in the event of an IED or VBIED, rules regarding window size, namely a window-to-wall ratio of 15 percent, and walled compounds. These standards were incorporated into legislation with the Secure
Embassy Construction and Counterterrorism Act of 1999. This act outlines five crucial security criteria with respect to embassies, which address blast resistant design and construction:

1. 100-foot setbacks from streets and uncontrolled areas to mitigate the impacts of a VBIED or IED.
2. High-perimeter walls and fences that are tough to climb, deterring would-be attackers on foot from entering the compound.
3. Anti-ram barriers to stop vehicles from penetrating the facility perimeter, getting close to the building, and detonating a VBIED.
4. Blast-resistant construction techniques and materials, e.g., reinforced concrete and steel construction and blast-resistant windows.
5. Access control of pedestrians and vehicles at the perimeter of a compound.95

Domestically, there were no standards for protective security measures of non-military federal buildings in America prior to the 1995 Oklahoma City Bombing.96 Following the attack, President Clinton tasked the Department of Justice (DOJ) with undertaking an assessment of the vulnerability of non-military federal facilities to acts of terrorism and other forms of violence, and to develop recommendations for minimum standards. Two months after the bombing, the DOJ published its report “Vulnerability Assessment of Federal Facilities.”97 It proposed 52 minimum security standards, based on a building’s assessed security level (ranked from minimum security I through to V maximum security). It also recommended the establishment of an Interagency Security Committee (ISC).98 This concerted focus on the protection of buildings and general efforts to design out terrorism culminated with the passing of Executive Order 12977 in October 1995, and the creation of the ISC, which was given three key responsibilities, namely the establishment of policies for security in, and protection of, federal facilities, the development and evaluation of security standards and a strategy for ensuring compliance, and to take such actions as may be required to increase the quality and effectiveness of security and protection of federal facilities.99 Over the years, the ISC has modified and updated the General Services Administration’s (GSA’s) Draft Security Criteria and working with other key federal agencies has developed ISC Standards such as perimeter buffer zones, security of entrances and exits, and introducing innovative design features such as shatterproof glazing and reinforced plates, the latter predominantly used in the ceilings of underground and multi-story parking garages.100 Both the GSA and ISC documents are considered important in that they represent “the first attempt to truly integrate security into every facet of the design and construction of a facility…. Prior to these documents, security was generally an afterthought: the last item added and the first item cut from any typical project.”101 Similarly, prior to 1999, there were no common standards for force protection (anti-terrorism/protective security measures) in fixed Department of Defense facilities.102 The military and Department of Defense facilities adhere to Unified Facilities Criteria 4-010-01 2018, which provides minimum antiterrorism standards for buildings, ranging from planning to design to construction, and also includes modernization criteria.103

While these measures sought to counter and mitigate the impact of future terrorist attacks, they were mainly deployed at sites of federal interest, with little attention paid toward other critical infrastructure or locations where mass gatherings took place (i.e., crowded places).104 Indeed, “with very few exceptions, the government does not compel private owners to make security changes or upgrades to their properties. Private buildings must only respond to building codes.”105 In the aftermath of 9/11, the New York City Department of Buildings convened a task force to analyze the building code as it related to the terrorist threat. The task force made 21 specific recommendations for code, code administration, and code enforcement changes. It stipulated that all high-rise commercial buildings taller than 100 feet must install sprinkler systems within 15 years. It also requested that egress routes, including doors and
stairs, must be marked with photoluminescent materials, and buildings must maintain plans to evacuate occupants in all kinds of emergencies.\textsuperscript{106}

In the UK, following an observable shift in terrorist attack methods from disruptive attacks on critical infrastructure assets, to attacks on crowded places, a number of guidance documents have emerged from government task forces, designed to help organizations mitigate risks associated with a terrorist attack.\textsuperscript{107} Examples include the Home Office’s \textit{Protecting Crowded Places: Design and Technical Issues} and the Centre for the Protection of National Infrastructure’s design guide for hostile vehicle attack mitigation.\textsuperscript{108} The UK government, through its National Counter Terrorism Security Office (NaCTSO), has placed considerable emphasis on protecting crowded places, using the vehicle of the Protect strand of the UK’s counter-terrorism (CONTEST) strategy.\textsuperscript{109} NaCTSO has delivered a number of projects since its inception in 2002, including Project Argus, a testing and exercising initiative that aimed to enhance resilience in the face of terrorism in crowded places. Project Argus was launched in 2007 and designed to engage mostly private sector organizations through mechanisms such as the Counter Terrorism Security Advisor network. Project Griffin sought to increase awareness of terrorist threats and provide information to businesses on what to do in the event of a terrorist threat or an actual attack.\textsuperscript{110} It has produced a number of guidance documents for a range of sectors within the UK, including the night-time economy, cinemas and theatres, stadia and arenas, retail, education, places of worship, hotels and restaurants, major events, visitor attractions, commercial centers, and transport.\textsuperscript{111} Topics covered consist of managing the threat (e.g. suspicious items and good housekeeping), attack methodology (e.g. IEDs, VBIEDs, bomb threats, chemical, biological and radiological [CBR] attacks, unmanned aircraft systems (i.e. drones), and the use of a vehicle as a weapon). Also covered are aspects of physical security, such as security awareness, access control, perimeter, control rooms, building construction, evacuation, and procedures following lockdown and in protected spaces.\textsuperscript{112}

While these programs and guidance documents were mostly designed to inform the business communities of already existing crowded places, emphasis was also placed on the need to inform those developing new crowded places in the future. In 2010, the Royal Institute of British Architects (RIBA) released guidance for architects, planners, and engineers on designing for counterterrorism. It contends that “in considering counter-terror risk response, the concepts of proportionality, relevance and effectiveness are fundamental. There is no need to build fortresses to protect property and interests against the terror threat, nor necessarily even a requirement to install extensive (and expensive) physical barriers or bollards.”\textsuperscript{113} The RIBA guidance highlighted the most common considerations for reducing vulnerability to the threat when designing for counterterrorism in the built environment, namely these: access control (e.g. electronic swipe cards readers, ANPR, and vehicle security barriers), hostile vehicle mitigation measures (e.g. active and passive barrier systems), surveillance CCTV, reception, communications, stand-off (e.g. recommended distance of 100 feet between an IED or VBIED and the building), measures relating to air conditioning/air handling systems, and service areas (e.g. loading docks).\textsuperscript{114} The guidance also considers containing damage in the event of a VBIED with specific reference to glazed façades and noted that “while we emphasise efforts to prevent or deter any successful terrorist attack, one should acknowledge that should a charge be detonated, glass often causes more injuries than the explosion itself.”\textsuperscript{115} Two possible design solutions were offered in the RIBA guidelines: firstly, design the glazing not to break. However, RIBA noted that this would result in very thick glazing, which necessitates very strong structural supports back to the building frame, leading also to costly facades, which is not a realistic option for most buildings. Secondly, design glazing that retains the glass fragments after the glass cracks, for example PVB laminated glass for new constructions or the application of anti-shatter film to existing glazing.\textsuperscript{116}

Collaboration between the Home Office and the Department for Communities and Local Government resulted in the publication of \textit{Crowded Places: The Planning System and Counter...}
Terrorism in 2012, which provides guidance to those involved in the planning, design, and development of crowded places.\textsuperscript{117} The guidance emphasizes four key counter-terrorism design principles aimed at deterring, detecting, and delaying a terrorist attack. First, designing better blast resistance (e.g., external barriers or a reinforced perimeter to prevent a penetrative or close proximity VBIED and the use of building materials that reduce fragmentation including blast resistant glass and a structural design which reduces the risk of building collapse). Second, designing better building management facilities (e.g., entrance arrangements which resist hostile entry and the separation of delivery areas and mailrooms from the main building). Third, designing better traffic management and hostile vehicle mitigation measures (e.g., structural measures that prevent unscreened vehicles gaining access to or coming into close proximity to the building and measures that reduce the speed of vehicles approaching the site like bends or chicanes). Finally, designing better oversight (e.g., clear lines of sight around the building, well maintained and litter-free environments that reduce the opportunity for placing and hiding suspicious items). It also recommended CCTV and the use of security guards, to provide formal oversight so that suspect activity could not go unnoticed.\textsuperscript{118}

Conclusion

From the discussion above, it is evident that there is a considerable body of knowledge with respect to protective security measures, including those aimed at preventing terrorist bomb attacks. Many of the measures utilize situational crime prevention techniques, and, as such, they are concerned with how a terrorist attack is committed, rather than why terrorism occurs. Thus, the measures aim to increase the effort, increase the risk, and reduce the rewards of the terrorist through target hardening and strengthening and utilizing a layered approach to security, based on deterring, preventing, protecting, and containing the threat. Historically, this has led to a degree of militarization and fortification of urban spaces and the creation of security zones in cities targeted by terrorists, such as Baghdad, Belfast, London, New York, and Washington, DC characterized by “rings of steel,” concrete barriers, and bollards. This has given rise to calls to consider a “balance between security aspects and other aspects of landscape design…. to achieve effective risk reduction without losing the identity of a building’s surrounding spaces.”\textsuperscript{119} The new American embassy in London is an example of this shift towards protective security measures that are acceptable to the public, aesthetically pleasing, and less obtrusive.

In her study on soft target hardening, Hesterman observed that in the US only “a very small portion of our national security budget and effort is spent protecting civilian venues.” Hesterman continues by saying that “Responsibility for security is often passed on to owners and operators, who have no training and few resources. In military terms, we are leaving our flank exposed.”\textsuperscript{120} Likewise in the UK, Lord Harris, in his review of how best to protect crowded places from a terrorist attack in 2007, acknowledged “that whilst a substantial amount of work had been undertaken to increase levels of protective security, more was needed to turn available advice into action on the ground.” According to Lord Harris, “A key finding was to highlight the importance of engaging with a wide range of local partners, in particular, local authorities and local businesses, to implement counter-terrorist protective security advice.”\textsuperscript{121} Despite the abundance of advice and guidance on offer, much of it is advisory not mandatory.

In the UK, in the aftermath of the Manchester Arena suicide bomb attack of May 2017, there has been a growing demand for greater protective security at public spaces and venues, culminating in the call for Martyn’s Law, named after Martyn Hett, one of the persons who lost his life in the attack.\textsuperscript{122} In February 2020, the Security Minister James Brokenshire announced plans to introduce a Protect Duty Law, that would make it mandatory that owners and operators of public spaces and venues consider the risk of a terrorist attack, and take
proportionate and reasonable measures to prepare for and protect the public from such an attack.\textsuperscript{123} The government’s consultation scheduled for the spring of 2020 has been delayed due to the COVID pandemic.\textsuperscript{124} Thus, as Meyer notes “the existing literature on protective security measures focuses mainly on suggesting measures for protecting targets against terrorism rather than on prioritizing such measures.”\textsuperscript{125}

\textit{Rachel Monaghan is Professor of Peace and Conflict at the Centre for Trust, Peace and Social Relations at Coventry University. Her research interests focus on political violence, informal justice, single-issue terrorism, counter-terrorism and crime and insecurity. She has been researching animal rights extremism for 30 years and has published articles on the subject in Terrorism and Political Violence and Studies in Conflict & Terrorism. She is Co-Editor of the journal Behavioral Sciences of Terrorism & Political Aggression and is currently the President of the Society for Terrorism Research.}

\textit{David McIlhatton is a Professor of Protective Security and Resilience, and the Director of the Institute for Peace and Security at Coventry University. He has published widely on counter-terrorism and is on a number of editorial boards of international peer-review journals and also reviews for multiple terrorism journals. His research portfolio includes projects with a value of over £17 million in security and business-related research areas internationally. He has been awarded with numerous international prizes for research excellence and was nominated to the Royal Society of the Arts as a result of his work in human security. He is also a Visiting Scholar at the University of Central Oklahoma.}
Endnotes


3 Meyer 2012, p. 310.


9 Clarke, 2017, p. 287.

10 For more details, see Arizona State University Center for Problem-Oriented Policing, 25 Techniques of Situational Crime Prevention. Available at: https://popcenter.asu.edu/content/learning-center


14 Wilkinson, Paul, Terrorism and the Liberal State. London: MacMillan, 1977. Wilkinson notes that for flights originating in North America there were 29 hijackings in 1971 and in 1972 but only 2 in 1973, the year after the security measures were introduced.

15 Reppetto, 1976, p. 166.


17 Ibid, p. 171. Clarke and Weisburd argued that two processes were at work in relation to diffusion, namely deterrence and discouragement. They suggested that as a crime prevention program in an area becomes known, would-be offenders’ uncertainty about the extent of the increased risk (deterrence) together with an exaggerated perception that the rewards of particular crimes are no longer proportionate with the effort (discouragement) leads to less crime.


22 Clarke and Newman 2006, p. 4. The application of SCP to terrorism is not without its critics; see Fussey, Peter, ‘Deterring Terrorism? Target–hardening, Surveillance and the Prevention of Terrorism’; in: Andrew Silke (ed.), The Psychology of Counter-Terrorism. London: Routledge 2011, pp.164-185. Fussey noted that such analyses “….largely assume a fairly straightforward application of crime prevention strategies to counter-terrorism and arguably overstate the similarities of these activities” (p. 164).

23 Boba 2009.


25 Ibid., p.136.


27 Ibid., p. 448.


30 Ibid.

31 Morris, Nancy A. ‘Target Suitability and Terrorism Events at Places’, Criminology & Public Policy, Vol. 14, No. 2, 2011. Morris further notes “that the existing evidence examining displacement and transference in terrorism was done so indirectly, and it has not examined whether target-hardening tactics have led to more attacks directed at similar targets in the surrounding geographic areas” (p. 421). 


33 Hsu, Henda Y. and David McDowall, ‘Does Target-hardening Result in Deadlier Terrorist Attacks against Protected Targets? An Examination of Unintended Harmful Consequences’, Journal of Research in Crime and Delinquency, Vol. 54, No. 6, 2017. The Global Terrorism Database (GTD) is an open-source database including information on terrorist events around the world since 1970. It is housed at the National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland.

34 Ibid., p. 945.


36 Hsu and McDowall 2017, p. 946.

37 Ibid., p. 931.


39 Meyer 2012, p. 313.


44 Ibid., p. 272.


46 For more details on the evolution of aviation security and Al-Qaeda plots against the aviation targets, see Hastings and Chan 2013, pp. 785-789.

47 Atlas and DiGregorio 2013. Blow out walls are designed to give during an explosion and let escape the positive pressure resulting from the blast.


50 Young, Carl S., *The Science and Technology of Counterterrorism*. Oxford: Butterworth-Heinemann, 2015, p. 133. For Davis, the car bomb “was comparable to airpower in its ability to knock out critical urban nodes and headquarters as well as terrorize populations of entire cities” (p. 5) – see Davis, Mike, *Buda’s Wagon: A Brief History of the Car Bomb*. London: Verso, 2007.

51 Young 2015, p. 135.

52 Little, Richard A., ‘Holistic Strategy for Urban Security’, *Journal of Infrastructure Systems*, Vol. 10, No. 2, 2004; Bennett 2018; Remennikov and Carolan 2005: Remennikov and Carolan suggest that maximizing stand-off distance “is the easiest and least costly method for achieving the appropriate level of protection to a critical structure” (p. 8).


57 Fussey 2011, p. 171. Intelligent pedestrian surveillance involves software designed to automatically spot ‘suspicious’ behavior or packages and bring it to the attention of CCTV operators.

58 Young, 2015.


64 Ibid.


66 Eytan, 2005.


68 Eytan, 2005.


71 Ibid., p. 32.


74 The Green Zone was installed in central Baghdad by the American military in 2003 and only re-opened to the public in 2019 - For more details see Daughtry, J. Martin, *Listening to War: Sound, Music, Trauma, and Survival in Wartime Iraq*. Oxford: Oxford University


Coaffee 2004; and Coaffee, Jon, ‘Recasting the “Ring of Steel”: Designing Out Terrorism in the City of London’; in: Stephen Graham (ed.), Cities, War, and Terrorism. Oxford: Blackwell Publishing, 2004, pp. 266-296. The Provisional IRA detonated two large VBIEDs in the City of London’s financial district in 1992 (Baltic Exchange bombing) and in 1993 (Bishopsgate bombing). The group also targeted London’s Docklands, the city’s second financial district in November 1992 but the VBIED was spotted by security guards. The area was targeted again in 1996 when a large VBIED detonated at the South Quay Station of Canary Wharf.


Briggs, 2005, p. 77. Following 9/11, concrete barriers were placed outside the Houses of Parliament in London and have since been painted black to make them appear less unwelcoming.

90 Coaffee et al., 2009, pp. 498-499. Collapsible pedestrian pavements also known as ‘Tiger Traps’ are designed to allow pedestrians to walk over them but give way under the weight of a vehicle thereby trapping the vehicle some way from the intended target. There is a ‘tiger trap’ outside the New York Mercantile Exchange. Other examples of covertly embedded features within London’s urban landscape include security balustrades at Whitehall and the use of reinforced letters spelling out Arsenal, benches and large canons dotted around Arsenal Football Club’s stadium.


92 Ibid, p. 111. Hidden measures include steel and concrete bollards within hedges, ditches deep enough to stop a truck, a wall of seating and benches atop of truck-impeding concrete.


95 Ibid.


102 This was a finding of the 1996 Downing Commission report on the Khobar Towers bombing in Dhahran, Saudi Arabia in 1996, which saw a VBIED bomb estimated to contain the equivalent of 3,000 - 8,000 lbs of TNT explode outside the northern perimeter of a facility housing American and allied forces supporting the coalition air operation over Iraq. The explosion resulted in 19 fatalities and some 500 injured persons. For more details, see Downing Assessment Task Force, Report of the Assessment of the Khobar Towers Bombing, 1996. Available at: https://fas.org/irp/threat/downing/annx_a.html.


107 Harris, Lord Toby, ‘London and Anti-terrorism in Europe’, European View, Vol. 16, 2017; Aradau, Claudia, ‘Crowded Places are Everywhere we go’: Crowds, Emergency,
Politics’, *Theory, Culture & Society*, Vol. 32, No. 2, 2015; and McIlhatton, David et al. 2019, pp. 44-45. Aradau notes “crowded places have recently been problematized as objects of terrorist attacks” (p. 155).


109 CONTEST involves the 4Ps, namely Pursue (i.e., to stop terror attacks from happening), Prevent (i.e., to stop individuals from either supporting or becoming terrorists), Protect (i.e., to increase protection from a terrorist attack), and Prepare (i.e., to mitigate the impact of a terrorist attack). For more details, see HM Government, *CONTEST: The UK’s Strategy for Countering Terrorism*, July 2011. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97994/contest-summary.pdf. The Protect strand of CONTEST focuses on keeping people safe by strengthening protection against terrorist attacks in the UK and its interests overseas, thus reducing vulnerability. It includes work undertaken to secure the Critical National Infrastructure, assessing and reducing risks to crowded places through improved protective security and strengthening UK border security.


111 These individual guidance documents have been collated into just one – see National Counter Terrorism Security Office, *Crowded Places Guidance*, Crown Copyright, 2017.


114 Ibid, p. 11.


116 Ibid.


118 Ibid., pp. 6-7.


Bibliography


Arizona State University Center for Problem-Oriented Policing, *25 Techniques of Situational Crime Prevention*. Available at: https://popcenter.asu.edu/content/learning-center.


Hooper, Ryan, “‘Martyn’s Law’ plan to protect public at venues is delayed by coronavirus’, Belfast Telegraph, May 21, 2020. Available at:


Web-based Resources

Arizona State University Center for Problem-Oriented Policing. Available at: https://popcenter.asu.edu/
Centre for the Protection of National Infrastructure. Available at: https://www.cpni.gov.uk/
National Capital Planning Commission (security). Available at: https://www.ncpc.gov/topics/security/
Chapter 24

Prevention of Kidnappings and Hostage-Takings by Terrorists

Alex P. Schmid

This chapter will look into what can be done to prevent kidnappings and acts of hostage taking, focusing on the seizure phase and the negotiation phase, in which the prevention of loss of lives among the hostages becomes paramount. This chapter will present an overview of the recent and contemporary prevalence of kidnappings and hostage takings and the outcome of such acts of terrorism, based on two, partly overlapping, ITERATE datasets. In doing so, this chapter will utilize roughly 4,000 kidnapping and hostage taking incidents over a fifty-year period (1968-2018). This will be followed by a presentation of some of the best practices which have evolved over the years to prevent these crimes and, failing that, to prevent loss of lives during captivity with the help of smart negotiation techniques. Criminal and political acts of kidnapping and hostage-taking, local and transnational abductions, and barricade and non-barricade types have their own dynamics and are, therefore, not always comparable. Successful kidnappings (e.g. the kidnappers collected a ransom payment, obtained the release or exchange of prisoners, were granted safe departure, or gained publicity) can encourage imitations and become contagious, thereby trading short-term prevention of loss of lives for long-term higher future risks of further abductions. The chapter’s Appendix reproduces Al-Qaeda’s kidnapping manual while a bibliography lists the most important literature on the subject.

Keywords: hostage-taking, kidnapping, negotiation, prevention, ransom, victims
Acts of terrorist aggression include (suicide) bombings, armed attacks on groups of people by assault rifles or missiles, arson attacks, individual or serial murder, and hijackings and other acts of hostage taking and kidnapping. The majority of terrorist attacks (about 80 percent in the case of transnational terrorist incidents) are single-phased (like in an armed assault or bomb attack) while the remainder (about 20 percent of transnational terrorist incidents) are dual-phased.1 Single-phased incidents usually occur before first responders arrive at the scene: the shots were fired or the bomb had exploded. Dual-phase incidents are different. Kidnappings involve the unlawful apprehension and abduction of persons against their will, followed by their confinement, usually in an unknown or unreachable hideout for coercive bargaining in order to extort a ransom or force a third party (often a government) to act or abstain from acting in a certain way (e.g. the release of imprisoned terrorists). Such abductions are always criminal in nature, but often have a political component. Above all, they have a strong human component. As one American hostage wrote in his diary of the 325th day of his captivity in Colombia: “Kidnapping. The deliberate creation and marketing of human grief, anguish and despair.”2

Contrary to kidnappings, acts of hostage-taking involve the seizure of a group of persons (less often a single person) and detaining them, usually at a known location, while threatening to injure, mutilate or murder some or all of the hostages in an effort to seek compliance to demands addressed to a third party, usually a government. They are not uncommon in insurgent warfare. Common to both kidnappings and hostage takings is that the victims – whether targets of opportunity or specifically selected persons – are seized by abductors and kept in a location, while compliance with demands is expected in exchange for not hurting those held captive and the eventual release of (some of) them. If the location is known and terrestrial, the scene of crime will be surrounded by security forces and the result is a barricade hostage-taking situation. These siege situations differ in important ways from other acts of hostage taking, but statistics sometimes combine barricade situations non-siege types of hostage taking. Locations for all types of hostage taking can be on land (e.g. embassy occupation), on water (e.g. piracy) or in the air (e.g. hijackings). This chapter only deals with terrestrial kidnappings and acts of hostage taking (for skyjackings and attacks on other transportation targets, see chapter 26 authored by Brian M. Jenkins). Its main focus is on kidnappings carried out by terrorists rather than purely criminal abductions. The latter constitute the large majority of kidnappings although they receive far less attention than those by terrorists.

The main strength of the kidnappers and hostage-takers stems from the element of surprise: for a brief moment in time, numerically weak terrorists can establish superiority of force at the scene of crime. In the case of kidnappings and hostage-takings, time stretches while surprise diminishes - at least in those cases where the location of victims and perpetrators is or becomes known (such as in a barricade siege situation where the hostages use their victims as human shields). Incidents are brought to a conclusion in various ways: negotiations, paying ransom, making political or other concessions, surrender, storming of a hostage site, or the death of perpetrators and/or victims - or a combination of these.

The threat to mutilate or kill one or more hostages if demands are not met by a deadline amounts to blackmail. It also leads to crisis situations where quick life-or-death decisions have often to be made under duress by local crisis negotiators, national governments, hostage negotiators, or other stakeholders. There is considerable variation in hostage takings and kidnappings. For instance, a bunch of armed men might enter a hut in a rural village at night and demand from the parents that their only son joins them for their holy struggle, threatening, in case of refusal, that they would take their daughters with them – a case of coercive extortion for recruitment typical for terrorist organizations like the Lord’s Resistance Army in Uganda or Boko Haram in Nigeria.3

How can such a kidnapping be prevented? The short answer in the case just mentioned is: it cannot be prevented. However, there are other kidnappings and acts of hostage-taking where
a more hopeful answer is possible, depending on such parameters as location, preparedness, and intelligence. A study of nearly 2,000 acts of transnational hostage takings showed that the hostage-takers were successful in capturing the hostages in 82.1 percent of the cases while for kidnappings the success rate of the perpetrators was 75.3 percent. While these are not very comforting figures, the situation is better when one looks at the survival of those taken hostage or kidnapped following negotiations. Here the respective figures for a successful release of those held are hope-giving, especially in the case of hostage barricade situations where the site of crime is surrounded by security forces. Much depends on the rationale behind an act of hostage taking or a kidnapping: is the objective money, political concessions, forced recruitment or sexual slavery? Terrorists also abduct people for publicity and propaganda purposes, for obtaining secret intelligence from the abductee, or a combination of any of these motives.

Prevention is possible when an attack is still in the planning stage, provided precise intelligence is available. More difficult is prevention in the seizure and abduction stage as the terrorists have the element of surprise on their side. Once the hostages are in the hands of the terrorists and kept in a known location - or brought to an unknown hideout - a negotiation process usually ensues. In this situation prevention means prevention of further harm by achieving the safe release of those kept against their will through skillful negotiation techniques involving some concessions.

In the following pages this chapter will sketch the wider picture of kidnapping and hostage taking before returning to the issue of prevention. Kidnappings and hostage takings other than the more overt barricade siege situations are difficult to investigate and those who know most about it are often the least likely to write candidly on the topic. As one insider to the negotiation business told the present author, when he invited him to write this chapter based on his first-hand experience with criminal and political, secular and religious hostage-takers:

“Terrorist kidnappings are an issue that is practically impossible to accurately research from open sources, because what you read is in most cases a crafted legend, and not the real story. The people who were involved will never write about it, as there’s is nothing to be gained by that - client confidence and strict confidentiality is paramount in this business, and no one wants to be seen as sharing information that might be useful to kidnappers. Then there is the issue of ransoms, which people claim to not have paid, but in reality, terrorists never release hostages for free.... There is also the issue of underreporting, and excessive focus on the rare cases of kidnappings of Westerners, rather than locals, who are kidnapped on a much more regular basis. As a result, most academic analyses of the KFR [Kidnapping for Ransom] phenomenon are completely off the mark ....”

Kidnappings and Hostage Takings – General Background

In the following section, part of the information on kidnappings and hostage takings is derived from information obtained from the ITERATE database, as reproduced in a 2010 study by Alex P. Schmid and Peter Flemming on the one hand, and in a 2020 study by Wukki Kim, Justin George, and Todd Sandler on the other hand. While these data refer only to transnational incidents, and while some of these go back in time to the late 1960s, many of the findings are still relevant and also apply to national incidents where both perpetrators and victims are local persons. The first article was based on an analysis of 1,904 incidents in the period 1968-2005, while the second is based on 1,974 - partly overlapping- incidents which took place from 1978 to 2018. Four types of transnational incidents are covered by the ITERATE data:
1. non-aerial hijackings: 3.3 percent in the period 1978-2006, 0.9 percent in the period 2007-2018;
2. barricade and hostage takings: 7.9 percent in the first period; 3.9 percent in the second period;
3. skyjackings: 17.8 percent in the first period, 4.1 in the second period;
4. kidnappings: 71 percent of total incidents in the first period; 91.2 percent in the second period.9

A quick comparison of the two periods suggests that preventive measures against skyjackings, especially after the 9/11 incidents, have significantly contributed to the reduction of aerial hijackings. On the other hand, kidnappings, mostly linked to the extortion of money, increased from just over 70 percent to more than 90 percent in the same period. Since 1992, kidnappings have become the main type of hostage events and represent a major source of income for many terrorist groups.10 As many kidnappings – especially the purely criminal ones – go unreported, figures about how widespread kidnappings are vary greatly. One report of the Swiss-based ETH Centre for Security Studies from 2013 noted that “… reliable statistics on hostage-takings and ransom payments are not available. According to estimates, between 12,000 and 30,000 kidnappings are carried out every year around the world, with the number of abducted foreigners in particular on the increase.”11

The financial rewards and the success rates of kidnappings in transnational incidents are probably the main incentives behind this form of crime.

Rukmini Callimachi, a reporter for the New York Times, noted on 29 July 2014:

“While European governments deny paying ransoms, an investigation by The New York Times found that Al Qaeda and its direct affiliates have taken in at least $ 125 million in revenue from kidnappings since 2008, of which $ 66 million was paid just last year.(…) And the business is booming: While in 2003 the kidnappers received around $ 200,000 per hostage, now they are netting up to $10 million, money that the second in command of Al Qaeda’s central leadership recently described as accounting for as much as half of his operating revenue.(…) In a 2012 letter to his fellow jihadists in Africa, the man who was once Bin Laden’s personal secretary,…[wrote]: “Thanks to Allah, most of the battle costs, if not all, were paid from through the spoils,” wrote Nasser al-Wuhaysi, the leader of Al-Qaeda in the Arabian Peninsula. “Almost half the spoils came from hostages.”12

In 2004, Al-Qaeda developed its own kidnapping manual which is reproduced in full as an Appendix to this chapter. Since paying ransom allows further terrorist attacks, one way of preventing kidnappings and other acts of hostage-taking would be to refuse to pay money to terrorists. The US and the UK have official no-concession policies. However, that has not spared citizens from these countries from being abducted and killed. One American study from 2017, investigating the question whether to pay or not to pay ransom money, reached two primary conclusions:

“First, countries that do not make concessions experience far worse outcomes for their kidnapped citizens than countries that do. Second, there is no evidence that American and British citizens are more protected than other Westerners by the refusal of their governments to make concessions.”13

What makes kidnappings and hostage takings so tempting for both ordinary criminals and political terrorists is that chances of managing to seize hostages as planned (what is termed
‘logistical success’) are high. Obtaining at least part of what they seek in the ensuing bargaining for the release of the hostages (what is termed ‘negotiation success’) is also quite high. According to ITERATE data analysed by Kim et al, “On average, hostage takers achieve logistical and negotiation (mean) success rates in 82.1% and 27.1% of incidents, respectively. (...) Kidnappings constitute 75.3% of logistical success and 81.1% of negotiation success relative to non-kidnappings.”

While purely criminal kidnappings for ransom – especially the local-to-local variant whereby both perpetrators and victims are from the same country - are much more frequent than terrorist kidnappings, the two forms sometimes overlap, e.g. when criminal abductors kidnap a high-profile person in order to sell the abductee to a terrorist organization which, in turn, seeks to obtain political concessions from a local or foreign government. In terms of modus operandi, there is also overlap in the way victims are selected and abducted. While there is evolution in tactics based on technology (e.g. regarding the ability of tracing a person’s whereabouts via mobile phone signals, or the payment of ransom in bitcoins), some things have not changed much in recent years (e.g. basic negotiation tactics). Therefore, some of the data presented below, reaching back more than forty years, are still of value. However, it has to be stressed that criminal and political acts of kidnapping and hostage-taking, local and transnational abductions, and barricade and non-barricade types have their own dynamics and are, therefore, not always comparable. Here then are some illustrative statistics, depicting duration of incidents, perpetrators, and victims.

Length of Hostage Ordeals

Kidnappings and acts of hostage taking are, as mentioned earlier, dual phase incidents. They can stretch out over days, weeks and months as the Table 1 makes clear.

Table 1. Duration of Incidents, 1978 - 2005

<table>
<thead>
<tr>
<th>Duration of Incidents</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than one week</td>
<td>20.2</td>
</tr>
<tr>
<td>One week to one month</td>
<td>13.3</td>
</tr>
<tr>
<td>One month to one year</td>
<td>10.5</td>
</tr>
<tr>
<td>Greater than one year</td>
<td>10.8</td>
</tr>
<tr>
<td>Irrelevant</td>
<td>23.3</td>
</tr>
<tr>
<td>Unknown</td>
<td>21.8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

An example of a long hostage incident was the storming and occupation of the US Embassy in Tehran on 4 November 1979. During this siege, 52 American diplomats and citizens became “guests of the Ayatollah” for 444 days, before being released on 20 January 1981, the same day on which Ronald Reagan became the US’ 40th president. Criminal kidnappings tend to be shorter than political ones, especially if the person kidnapped has anti-kidnapping insurance and the support of a professional hostage negotiator. According to Control Risks, a London-based firm which offers its services for kidnapping negotiations, 80 percent of all kidnappings it recorded in 2019 lasted less than one week, while 6 percent lasted longer than four weeks. The duration of being held in captivity affects the mood of the hostages. In their confinement
victims often experience helplessness, hopelessness, powerlessness, worthlessness, bewilderment, frustration, anxiety, despair, and stress due to their fear of death. Especially in cases of long detention periods, the post-release effects of captivity tend to lead to long-lasting trauma.20

Perpetrators
Survival chances for those abducted and held in captivity depend on the type of kidnappers and hostage takers. There is a considerable variety in perpetrators, as the following typology makes clear. Irvin Goldaber identified nine categories of hostage takers.

Table 2. Typology of Hostage-takers21

<table>
<thead>
<tr>
<th>Type of hostage taker</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suicidal person</td>
<td>wants someone else to fulfil his death wish</td>
</tr>
<tr>
<td>Vengeance seeker</td>
<td>wants to gain revenge</td>
</tr>
<tr>
<td>Disturbed individual</td>
<td>wants to achieve mastery and solve his problem</td>
</tr>
<tr>
<td>Cornered perpetrator</td>
<td>wants to effectuate escape</td>
</tr>
<tr>
<td>Aggrieved inmate</td>
<td>wants to obtain freedom or bring about situational change</td>
</tr>
<tr>
<td>Felonious extortionist</td>
<td>wants to obtain money</td>
</tr>
<tr>
<td>Social protestor</td>
<td>wants to bring about social change or obtain social justice</td>
</tr>
<tr>
<td>Ideological Zealot</td>
<td>wants to redress a grievance</td>
</tr>
<tr>
<td>Terrorist Extremist</td>
<td>wants to obtain political change</td>
</tr>
</tbody>
</table>

This list is incomplete, as it excludes incumbent rogue state actors as well as insurgents and guerrilla movements (which can be designated terrorist organisations) engaged in civil wars. While state-sponsored international abductions are rare, domestic hostage taking in civil wars are not. Prisoners of war are sometimes kept as hostages and used for prisoner exchanges. However, in these cases they are usually not treated according to the rules of international humanitarian law. Non-combatants are sometimes also seized to create terror and submission. A major example of the use of abductions by insurgents are the Revolutionary Armed Forces of Colombia (FARC). A recent fact-finding report on the FARC described:

“…. hitherto undisclosed details of the conditions in which the FARC kept some of the 21,396 hostages they took from 1990 to 2016. The guerrillas who claimed to be fighting for a more just society, seized rich and poor alike. They beat and starved the hostages. Many were forced to urinate in their clothes and not allowed to clean themselves for months. Some were locked in wooden boxes barely larger than their bodies. The rebels ordered some to dig their own graves as a form of psychological torture.”22

Other terrorist groups, e.g. Boko Haram in Nigeria, kidnap young men and women in schools and dormitories not just for ransom, but also for sexual slavery or for fatal operational tasks – coercing some of them to become suicide bombers.23 The Nigerian government has paid ransom for the release of abducted girls in high profile cases and also provided the rebels with vehicles as part of secret deals it made. Boko Haram’s mass abductions have forced hundreds of thousands of people to flee north-eastern Nigeria.

Types of Victims
When it comes to the prevention of kidnappings and acts of hostage taking, it is, first of all, important to know who is likely to become a victim. As Table 3, based again on ITERATE data covering transnational incidents only, makes clear, about half of the victims were ‘private parties’ while about one-fifth were corporate officials with most of the others either being local or foreign government officials. The latter are often “protected persons” – protected by kidnapping insurance which makes it more likely that they can be bailed out by a ransom payment.

Table 3. Type of Immediate Victims of International Hostage Incidents 1968 - 2005

<table>
<thead>
<tr>
<th>Type of Immediate Victim</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host government officials</td>
<td>33</td>
<td>1.7</td>
</tr>
<tr>
<td>Foreign diplomats or official, nonmilitary</td>
<td>295</td>
<td>15.5</td>
</tr>
<tr>
<td>Host government military</td>
<td>14</td>
<td>0.7</td>
</tr>
<tr>
<td>Foreign military</td>
<td>75</td>
<td>3.9</td>
</tr>
<tr>
<td>Corporation officials</td>
<td>400</td>
<td>21.0</td>
</tr>
<tr>
<td>Prominent opinion leaders</td>
<td>88</td>
<td>4.6</td>
</tr>
<tr>
<td>Private parties</td>
<td>960</td>
<td>50.4</td>
</tr>
<tr>
<td>Suspected terrorists</td>
<td>12</td>
<td>0.6</td>
</tr>
<tr>
<td>Indeterminate</td>
<td>27</td>
<td>1.4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1,904</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

The harsh truth is that a broad range of persons can become victims of kidnappings and hostage taking. However, the lethality of kidnappings and acts of hostage-taking, when compared to the one of other types of terrorist incidents, is less in terms of total fatalities (Table 4). In the case of barricade situations, victims were sometimes killed when government troops tried to storm the hostage site (e.g. in Beslan, North Ossetia, 2004). However, there have also been cases where the hostage takers came to kill rather than negotiate and found themselves surrounded by security forces before they could escape (e.g. Westgate, Nairobi, 2013).

Table 4. Fatalities per Attack across Tactics, 1970-2014 (N = 113,770)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Tactic</th>
<th>Fatalities per Attack</th>
<th>Total Fatalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Hijacking</td>
<td>7.80</td>
<td>3,635</td>
</tr>
<tr>
<td>2.</td>
<td>Armed assault</td>
<td>4.19</td>
<td>126,967</td>
</tr>
<tr>
<td>3.</td>
<td>Hostage-taking (barricade)</td>
<td>2.45</td>
<td>1,627</td>
</tr>
<tr>
<td>4.</td>
<td>Bombing/explosion</td>
<td>1.62</td>
<td>85,271</td>
</tr>
<tr>
<td>5.</td>
<td>Assassination</td>
<td>1.36</td>
<td>20,473</td>
</tr>
<tr>
<td>6.</td>
<td>Hostage-taking (kidnapping)</td>
<td>1.25</td>
<td>7,938</td>
</tr>
<tr>
<td>7.</td>
<td>Unarmed assault</td>
<td>1.07</td>
<td>505</td>
</tr>
<tr>
<td>8.</td>
<td>Facility/infrastructure attack</td>
<td>0.77</td>
<td>6,031</td>
</tr>
</tbody>
</table>

Note: Attacks that used more than one tactic are included in this table for each tactic (2,688 attacks with unknown tactics are excluded).

There are various types of kidnappings and abductions and prevention is hardly possible in some of them. To give four examples:
1. *Express kidnapping*: “Express kidnapping,” for instance, as are frequently reported from Mexico, involve the abduction of a person on the street or in a taxi and holding that person until he or she has emptied her or his own bank account from publicly accessible ATM machines and handed all the money over to the kidnappers. Express kidnappings last only as long as there is money on the bank account and then the robbed person is normally drugged and released unharmed at some desolate place.

2. *Miracle fishing*: Another type of abduction, popular in Colombia, was “miracle fishing” (Pesca Milagrosa): erecting illegal roadblocks in a rural area, using fake police or military uniforms in order to stop busses and cars and force the travellers out of the vehicles for identity card controls. Some of them are “arrested” after having been assessed for their likely ransom worth. The perpetrators take the most promising ones into captivity, the end result being a regular kidnapping. The poor-looking travellers are allowed to continue their journey.26

3. *Enforced disappearances*: Yet another form of abduction are so-called (enforced) “disappearances.” Victims, usually political activists, are snatched at their homes or at their workplaces or on the way between these places by plainclothes state agents, brought to a secret prison, tortured and finally disposed of, e.g. by dropped them, with arms and legs tied, from a helicopter into the high sea, as happened in Argentina in the 1970s.27 In recent years, the Syrian government has used the tactics of disappearances in more than ten thousand cases against suspected enemies of the Assad regime.

4. *Tiger kidnappings*: Yet another form of kidnapping is so-called “Tiger kidnappings.” One of more family members e.g. parents, children) are abducted and kept in captivity until another family member (e.g. a father or son) has committed a crime on behalf of the kidnappers – e.g. placing a car bomb in a location to which that person has easy access while the kidnappers themselves have not. This tactic was used by the Provisional IRA in Northern Ireland in the 1990s.28

These particular types of kidnappings and abductions are hard, if not impossible, to prevent. In the following sections we will explore what can be done in terms of prevention and preparedness, focussing on two points in time: prevention of being abducted and held by the captors and prevention of being harmed in the course of a hostage detention situation. We will explore each of these two scenarios in turn.

**Prevention in the Planning and Abduction Phase**

Most of the existing guidelines about what a person in danger of being kidnapped can do to prevent being taken hostage refer to other types of kidnapping than the four sketched above. These guidelines usually focus on high-level expatriates (e.g. diplomatic personnel and foreign businessmen) who live in unsafe countries and crime-ridden cities, but do not have personal round-the-clock protection from armed bodyguards like ambassadors or corporate chief executive officers. However, some of the recommendations formulated for these expats are also useful for ordinary citizens as well as for ordinary foreigner visitors.

Guidelines developed by the German Criminal Office (BKA) and distributed by EUROPOL offer, among other recommendations, the following measures that can be taken by a prospective victim.29 Preventive measures for those likely to become victims of abductions include:

- Developing security awareness
- Identifying your own vulnerabilities
- Be alert and observant
● Avoiding going to unsafe areas
● Avoiding providing criminals with opportunities
● Watching out for individuals or vehicles following you
● Keeping a low profile
● Avoiding routines, vary the time you depart for, and return from, work
● Varying your route and take detours
● On the road, avoiding stopping next to vehicles you cannot see into (like delivery vans)
● Being aware that unusual incidents, such as an injured person at the side of the road, may in fact be the cover of a trap.
● Knowing about exits, escape routes and safe places on your everyday routines
● Preventing being harmed in the abduction/capture phase.30

For the abductee the danger to life and limb is highest in the first hour of the kidnapping when the hostage-takers are nervous and aggressive, fearing the intervention of security forces or bystanders. To minimize being hurt or killed in that early detention phase, the same BKA/Europol guidelines suggest that victims follow these rules.

Preventive measures while in captivity:31

● If you cannot escape immediately and successfully, you must accept your situation for the time being.
● Try to gain control over your shock, fear and agitation by staying calm and following the instructions of the kidnappers/hostage-takers.
● Take a passive role, do not argue, do not make direct eye contact. Refrain from making accusations and appearing hostile or arrogant.
● Now your aim is to stabilise the situation. Try to establish a personal relationship with the offenders without going too far.
● Stay politically neutral. Avoid controversial issues such as religion or politics.
● Try to keep your dignity and self-respect.
● Do not negotiate with the offenders - this will be done by others. The offenders will make their demands to a third party.
● Follow the instructions of the offenders if you are allowed to make a phone call, even if they tell you to lie.
● Be patient. Do not give up and think positively! You can be assured that everything possible is being done for you.

Such instructions for the benefit of the victims ought to be juxtaposed by the instructions which the hostage-takers get from their organization. Their instructions indicate that the abductors are aware of the content of such victim protection guidelines. The reader can find those from Al-Qaeda’s kidnapping manual in the Appendix to this chapter. They make for sombre reading, making also clear that the hostages are considered mere bargaining chips – expendable human beings.

The first phase of kidnapping – seizure and abduction – is usually followed by a phase where little seems to be happening. The hostages are usually aware that negotiations are going on, that threats are issued and that an ultimatum has been set. In barricade siege situations a few hostages (e.g. women and children) might be released in return for food and drinks, but in other types of hostage taking, some hostages are sometimes mutilated or shot in order to put more pressure on the government to make concessions. Hostages can generally do little to improve their fate, but they can sometimes do something to prevent it from getting worse based on skills developed in survival trainings32 until a settlement or a rescue changes the circumstances. However, their fate is now in the hands of others.
Prevention of being Harmed and Killed in the Detention and Negotiation Phase

Once seized, the fate of those kidnapped or taken hostage is primarily in the hands of the perpetrators and the authorities opposing them. Both are eager to negotiate – or at least to communicate. Some countries, (e.g., the US, the UK, and Canada), have an official no-concession policy with terrorists. Nonetheless, there is almost always some form of communication taking place between a government and the terrorists. Although, no-concession policies are publicly upheld by many countries, several of them do not, in fact, adhere to this strategy, as they are making secret deals with the perpetrators, often with the help of a third party.

The negotiator is the liaison between terrorists and authorities. In barricade siege situations time is on the side of the authorities as negotiators can take turns. The hostage takers might take amphetamines or other drugs to stay awake and alert, but these drugs also tend to make them very volatile. As a consequence, the bargaining process can become highly emotional and less rational. If the government has no idea where hostages are, time tends to be on the side of the hostage-takers as long as the latter feel secure their location has not been compromised. For the hostages, the longer an incident lasts, the greater the post-traumatic stress tends to be for those who survive the ordeal.

Contrary to kidnapping situations where the kidnappers’ own lives are not in direct danger, in hostage-barricade situations the outcome of the negotiations – or of the breakdown of these – is a matter of life and death, not just for the hostages, but also for the hostage-takers. They are afraid of being targeted by snipers or surprised by a special assault forces and, therefore, often use the hostages as human shields. For instance, in the case of the 2004 Beslan school siege, one of the hostage-takers, Ruslan Khuchbarov, sent a hand-written note to the security forces surrounding the school: “If they kill any of us, we will shoot fifty people to pieces. If they injure any one of us, we will kill twenty people. If they kill five of us, we will blow up everything. If they turn off the light, even for a minute, we will shoot to pieces ten people.”

In combination with maximalist demands (in this particular case demands along these lines: “We insist that Putin immediately resigns from his post as President of the Russian Federation”), the task of the hostage negotiator is not an enviable one as he often has very little to offer which might soften the stance of the hostage-takers.

The negotiator (often a “he” since the hostage takers are generally males, but female hostage negotiators are also trained by Western governments although some jihadists might not want to deal with a female negotiator) is caught between intransigent terrorists and sometimes almost as intransigent authorities making his or her space for manoeuvring very small. The negotiator, while buying time, is on the one hand expected to put pressure on the hostage-takers and, on the other hand, keeping their hope alive that at least some of their demands are met. As mentioned, he or she is the liaison between the government and the terrorists, and often has nothing better than a phone line to analyse and judge the situation and make a decision on, if, and how to move forward in the negotiation process. If the negotiations are progressing well, the negotiator might notice that the hostage takers’ spokesperson speech is less excited and loud, that deadlines are allowed to pass without hostages being hurt or shot, and that some mutually satisfying outcome is within reach. On the other hand, if things tend to go wrong, he or she will notice language that has death as its main theme, not just for the hostages, but also for the hostage-takers. If the negotiator – or rather negotiators since it is usually a team effort of 4-5 experts – signals such a deterioration in a hostage-barricade situation to superiors, they might decide that a rescue operation by force might be the only option left.

Various guidelines for hostage negotiators have been developed. One of the more useful ones is based on interviews with professional negotiators, collecting their common wisdom.
They refer mainly to criminal hostage situations in the US and are based on the insights of 50 negotiators. This common wisdom on hostage negotiations is discussed in terms of percentage of hostage negotiators (n = 50) agreeing or strongly agreeing with the following statements:

- A key function in hostage negotiations is buying time while attempting to defuse the situation (100 percent).
- A hostage negotiator must be on the constant lookout for a “suicide ritual” by the hostage taker (100 percent).
- The main objective in a hostage situation is the preservation of human life, including that of the hostage takers (96 percent).
- The “Stockholm Syndrome” applies not only to hostages, but also to hostage takers and hostage negotiators as well (94 percent).
- The most dangerous time for hostages is the first minutes after being taken hostage (90 percent).
- In a hostage situation, it is important for the hostage negotiator to try to find a face-saving solution for the hostage taker (88 percent).
- The key to successful hostage negotiations is flexibility (86 percent).
- Nothing is owed to the hostage takers and if an opportunity to safely liberate the hostages becomes available, it should be taken (84 percent).

Negotiations with jihadist hostage takers in the 21st century ask for new measures. A very thoughtful set of principles for hostage negotiators that goes beyond traditional checklists like the one above, has been suggested by two seasoned hostage negotiators, Adam Dolnik and Keith Fitzgerald.

New Rules for Hostage-Barricade Situation Negotiations, by A. Dolnik and K. Fitzgerald:

- Always keep in mind that negotiation is not just about reaching “deals” and making quid pro quo exchanges; it is also about exercising influence over the thinking, behaviour, and decision making of others. Any information gained in conversation – and the very act of having the conversation itself – may present such opportunities at any time.
- Be (and remain) self-diagnostic: understand your own biases and constantly question your assumptions about the hostage takers, their motives, and their willingness to negotiate (keeping in mind that there is a big difference between self-diagnosis and self-doubt). Do not cling to conclusions out of frustration or disgust, or you will miss important clues and opportunities.
- Do not negotiate with the “terrorist,” negotiate with the rational human being who, for some set of reasons, has chosen – or felt forced into – an extreme, violent course of action.
- Use an active listening approach to the negotiations, not just a bargaining approach; focus at least as much on asking good questions, learning, and understanding grievances and motives as on making quid pro quo substantive deals.
- Ask for as many details as possible about the reasons/justification the perpetrators use to explain their actions. The answers will provide criteria that may be useful in other ways later.
- Look for empathetic ways to acknowledge or validate legitimate grievances behind the terrorists’ actions while differing with the action themselves. This will make it harder for them to label you as unreasonable, it will create chances to de-escalate the situation emotionally, and it may help you to create a wedge between their grievances and their actions, which in turn may help them to question the connection.
- Brainstorm with them. Rather than simply trying to stall with the “good cop, bad cop
routine”, genuinely look for ways to address the more legitimate grievances in ways that do not require unwise, unreasonable, or impossible concessions.

- Make sure someone is looking at the bigger picture, beyond the incident.38

Hostage negotiations require exceptional professional communication skills and cultural sensitivity. If the hostage negotiator does not manage to achieve a surrender or a solution requiring few concessions from the government, pressure to solve the situation by bringing in special forces to storm the hostage site will be mounting. Unfortunately, there is some statistical evidence that more hostages have been killed during rescue attempts than in cold blood by the terrorist themselves.39 To give an example: When Russian special forces tried on 3 September 2004 to liberate over 1,200 people (777 of them children) in a school in Beslan, (North Ossetia) 331 died on the third day when the special forces intervened, more than half of them (171) were children.40

However, the data on chances of survival for those held captive are not all bad. Much depends on the type and place of an abduction and the policy of the government in attempting to solve the crisis. In Western Europe, in particular, the outcome has been generally better, thanks to honed hostage negotiator skills and, perhaps as much if not even more so, thanks to the concessions made by governments. One study from the early 1980s, surveying 146 incidents of political hostage-taking in Europe over a twelve-year period found that 94 percent of the hostages were released, regardless of whether all demands were met or not.41

What can a skilful hostage negotiator do to prevent loss of lives? He or she has to be a non-judgmental listener and empathetic in the communication process. During the negotiations he or she has to build trust with the hostage takers and develop in dialogue with them a face-saving solution for both sides.42 However, the government must give the negotiating team something to bargain with. If the location of the hostage takers is encircled by security forces, the bargaining position of the negotiator is much better than in a kidnapping situation where the location of the hostages is not known. The negotiator can then suggest to the hostage takers that he is the only person that can prevent an assault. In exceptional cases, he might even be able to promise them a safe conduct– the so-called Bangkok solution named after an incident where four Palestinian Black September terrorists were granted a safe passage to Egypt in exchange for the release of the six hostages they had taken in the Israeli embassy in Thailand in December 1972.43 As the Table 5 makes clear, it is not a very frequent solution to hostage crises.

How many hostages survive their ordeal and are freed? That depends very much on the actor and the location. Given the fact that far from all cases are made public, it is difficult to make firm statements. The kidnapping negotiation and insurance industry keeps records and claims that in about 90 percent of cases the hostages are successfully ransomed.44 That figure might, however, be too optimistic since the majority of hostages cannot not afford insurance and many, perhaps the majority of hostage takings, especially the purely criminal ones, do not enter records and may never have been reported.45 With a fanatical organization like ISIS, hostage survival rates would be much lower than 90 percent while with many other groups, especially criminal groups, it may be closer to 95 percent – considering not only negotiated releases, but also escapes and rescues. As long as negotiations go on, it is rare for kidnap victims to get killed except when they try to escape or in failed rescue attempts. Yet the picture has many shades of grey between the black of death and the white of unharmed release as Table 6, based on the ITERATE database makes clear.

This table makes clear that prevention in the first phase – (7,8,14) amounts to 4.8 percent of all cases in transnational acts of kidnappings and hostage taking. However, prevention in the form of “Incident forestalled by authorities before initiation” (13) worked in another 1.8 percent of cases, bringing the total prevention score for phase one to 6.6 percent of 1,410 incidents of kidnapping and hostage-taking.
The success rate in the detention/negotiation phase is much better: Adding categories 1, 2, and 12, brings the total to a respectable 57.9 percent for the last phase.

Table 5. Types of Government Responses, 1978 - 2005

<table>
<thead>
<tr>
<th>Type of Response</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capitulation</td>
<td>53</td>
<td>3.8</td>
</tr>
<tr>
<td>Stalling, with compromise on demands</td>
<td>109</td>
<td>7.7</td>
</tr>
<tr>
<td>Bangkok solution</td>
<td>9</td>
<td>0.6</td>
</tr>
<tr>
<td>No compromise, no shootout with the perpetrators</td>
<td>190</td>
<td>13.5</td>
</tr>
<tr>
<td>Shootout with the terrorists</td>
<td>122</td>
<td>8.7</td>
</tr>
<tr>
<td>Government double-cross</td>
<td>3</td>
<td>0.2</td>
</tr>
<tr>
<td>Massive nationwide search, with no compromise</td>
<td>28</td>
<td>2.0</td>
</tr>
<tr>
<td>Irrelevant, negotiations were not established</td>
<td>533</td>
<td>37.8</td>
</tr>
<tr>
<td>Unknown, indeterminate</td>
<td>363</td>
<td>25.7</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1,410</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Table 6. Hostage Fate, 1978 – 2005, according to ITERATE data

<table>
<thead>
<tr>
<th>Fate of Hostage</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  No damage or casualties, hostages released, no capitulation</td>
<td>531</td>
<td>37.7</td>
</tr>
<tr>
<td>2  No damage or casualties, hostages released, capitulation or compromise</td>
<td>161</td>
<td>11.4</td>
</tr>
<tr>
<td>3  Victims killed, no target capitulation</td>
<td>102</td>
<td>7.2</td>
</tr>
<tr>
<td>4  Victims killed, capitulation or compromise by targets</td>
<td>1</td>
<td>.1</td>
</tr>
<tr>
<td>5  Damaged material, no target capitulation</td>
<td>1</td>
<td>.1</td>
</tr>
<tr>
<td>6  Victim killed while attempting escape after initial capture</td>
<td>2</td>
<td>.1</td>
</tr>
<tr>
<td>7  Victim successfully avoided capture</td>
<td>27</td>
<td>1.9</td>
</tr>
<tr>
<td>8  Victim successfully avoided capture after incident began</td>
<td>39</td>
<td>2.8</td>
</tr>
<tr>
<td>9  Hostages killed in shootout</td>
<td>20</td>
<td>1.4</td>
</tr>
<tr>
<td>10 Hostages killed, no provocation, during negotiations</td>
<td>21</td>
<td>1.5</td>
</tr>
<tr>
<td>11 Hostages killed during negotiations, deadline had passed</td>
<td>5</td>
<td>.4</td>
</tr>
<tr>
<td>12 Hostages rescued by authorities</td>
<td>124</td>
<td>8.8</td>
</tr>
<tr>
<td>13 Incident forestalled by authorities before initiation</td>
<td>25</td>
<td>1.8</td>
</tr>
<tr>
<td>14 Victim escaped after initial capture</td>
<td>1</td>
<td>.1</td>
</tr>
<tr>
<td>15 Irrelevant</td>
<td>6</td>
<td>.4</td>
</tr>
<tr>
<td>16 Unknown, indeterminate</td>
<td>344</td>
<td>24.4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1,410</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>
On the downside, the cases where hostages were killed by either terrorists, rescue forces, or in the crossfire between them (3, 4, 6, 9, 10, 11 in Table 10) add up to 10.7 percent of the 1,410 cases.

In sum, prevention in the first and the last phase of kidnappings and acts of hostage-taking add up to 64.5 percent – almost two thirds of all cases. However, these ITERATE figures are only referring to transnational terrorism and might not be representative for other types of kidnappings and hostage taking.

There is a dark, unknown side to that seemingly high success rate: where terrorists got away with a ransom, managed to release imprisoned fellow terrorists as the government made concessions, that money and those prisoners might be the source of new acts of kidnapping and hostage taking in the future. In addition, their “success” in obtaining high ransoms might inspire others to also enter the business of kidnapping and hostage taking.

Conclusion

In this chapter, we have identified two phases of kidnapping and hostage-taking where prevention is possible (though not easy). First, in the phase preceding the abduction/detention and, second, in the negotiation phase while hostages are being held in captivity. In the first phase, the potential victim is the main preventer. In the second phase it is the hostage negotiator, because he has the ability to save lives. However, in those cases where ransom was paid by governments and the killing of hostages could be prevented, some of the money obtained in this predatory crime is likely to be invested in organizing further kidnappings. In other words, conceding to the terrorists’ demands (i.e. paying ransom) might encourage terrorists to carry out more kidnappings and hostage takings. The contagiousness of kidnappings and acts of hostage-taking following successful abductions and after securing hefty ransoms is well documented.

However, the inclination to avert immediate and certain death of innocent people taken hostage is for governments, under the pressure of public opinion, – especially in liberal democracies – often greater than the desire to avert a higher risk of more acts of kidnapping and hostage-taking in the future. Deterrence of kidnappings and other acts of hostage-taking by denying concessions can be effective, but only in some cases. If the terrorists are not willing to negotiate, but only take hostages to murder them in front of rolling video-cameras (as in the case of some of ISIS’ acts of terrorism), there is little that can be done beyond admonishing the mass and social media not to broadcast such violence in vivid details. If terrorists are suicidal and wish to die accompanied by as many of their “enemies” as possible, deterrence does not work either. However, these are still exceptional situations rather than the rule.

Prevention is possible. However, successful preventive measures are not feasible without preparedness in the first phase of kidnappings and hostage-takings, or without professional negotiation skills and some room for manoeuvre for the negotiator in the final phase. Prevention is a remedy that always ought to be tried. There is often a price to prevention, especially when kidnapping insurance fees and ransom money are paid. That price might be high, but so is the life of an innocent human being facing a terrorist ultimatum.

In the second chapter of this volume, we distinguished between up-stream-, mid-stream, and down-stream prevention. In this chapter we have focused on the admittedly limited possibilities of downstream prevention. In terms of the mid- and upstream prevention, some of the broader counter-measures against terrorism discussed in chapter 2 might apply. Yet, their exact effect on downstream phenomena is hard and sometimes impossible to assess.

If we look at up- and mid-stream prevention measures not in terms of their presence, but their absence, the importance of these mid- and up-stream measures becomes clear. What
happens when the state breaks down and the bonds that hold societies together disappear, is illustrated by the events that took place in Chechnya in the late 1990s:

“Kidnapping in Chechnya was perpetrated by all segments of Chechen society: criminal gangs, clans, bandits and rebel groups, even top-level government officials were suspected of involvement. (…) However, this tradition [of historical hostage taking in Chechnya – APS] mutated into a new phenomenon during the first Chechen war of independence in 1996, as a result of the Russian Federation’s practice of detaining civilians for questioning. Described as ‘arbitrary detention and extortion’, detainees could be bought back by paying a ransom to Russian authorities. (…) The practice of buying civilian detainees was counterbalanced by exchanging captured federal soldiers. Often, Russian soldiers who were captured in battle were killed immediately only sparing a minority in order to sell for exchange. Hence, the relatives of a detainee could buy a federal soldier from a rebel group and then ransom him for their family member. Tishkov (2004) explained the process in which a family could visit a ‘hostage market’ and place an order to buy a captive. The families had the ability to choose in advance the category of hostage they required, whether it was a businessman, an officer, or a civil servant. (…) Extreme violence was a common feature in the Chechen negotiation process; kidnappers tortured or maimed hostages on video, by using various cruel methods of torture. (…) Typically, hostages were abducted by smaller criminal groups, valued and then sold along the supply chain to larger criminal or rebel organizations. Once the hostage reached the end of the supply chain, the commodities were then stored in purpose-built prisons equipped with torture chambers.”

Situations like these are exceptional, but have been approached in other places where foreign intervention and civil war nearly destroyed state and society; Iraq after the 2003 US-led invasion is a striking example hereof. Civil war, foreign intervention, absence of good governance, widespread corruption, economic misery, black markets, unpunished crime and lack of rule of law and human rights are some of the up- and mid-stream factors that are likely to contribute to down-stream kidnappings and acts of hostage taking.

Alex P. Schmid is a Research Fellow at the International Centre for Counter-Terrorism (ICCT) in the Hague, the Netherlands. He is Editor-in-Chief of Perspectives on Terrorism and former Co-Editor of Terrorism and Political Violence – both leading journals in the field of Terrorism Studies. Until 2009, Prof. em. Schmid held a chair in International Relations at the University of St. Andrews where he was also Director of the Centre for the Study of Terrorism and Political Violence (CSTPV). Previous positions include Officer-in-Charge of the Terrorism Prevention Branch of the UN Office on Drugs and Crime in Vienna and a chair in Conflict Resolution at the Erasmus University Rotterdam. Between 1978 and 2018 he also held various positions at Leiden University. Currently, he is Director of the Vienna-based Terrorism Research Initiative (TRI), a consortium of 16 institutes and more than 100 individual scholars seeking to enhance human security through collaborative research. Alex Schmid has more than 200 publication and reports in ten languages to his name, including the award-winning volume “Political Terrorism” (1984, 1988, 2006) and the “Routledge Handbook of Terrorism Research” (2011, 2013).

Authored by Abdel Aziz Al Moqrin

Kidnapping

Reasons for detaining one or more individuals by an enemy:

1. Force the government or the enemy to succumb to some demands.
2. Put the government in a difficult situation that will create a political embarrassment between the government and the countries of the detainees.
3. Obtaining important information from the detainees.
4. Obtaining ransoms. Such was the case with the brothers in the Philippines, Chechnya, and Algiers. Our brothers from Muhammad’s Army in Kashmir received a two-million-dollar ransom that provided good financial support to the organization.
5. Bringing a specific case to light. This happened at the beginning of the cases in Chechnya and Algeria, with the hijacking of the French plane, and the kidnapping operations performed by the brothers in Chechnya and the Philippines.

Requirements needed in forming a kidnapping group:

1. Capability to endure psychological pressure and difficult circumstances. In case of public kidnapping, the team will be under a lot of pressure.
2. Intelligence and quick reflexes in order to deal with an emergency.
3. Capability to take control over the adversary. The brother is required to possess fighting skills that will enable him to paralyze the adversary and seize control of him.
4. Good physical fitness and fighting skills.
5. Awareness of the security requirements, prior to, during, and after the operation.
6. Ability to use all types of light weapons for kidnapping.

Types of Kidnapping

Secret Kidnapping: The target is kidnapped and taken to a safe location that is unknown to the authorities. Secret kidnapping is the least dangerous. Such was the case of the Jewish reporter Daniel Pearl, who was kidnapped from a public place, then transferred to another location. It is also the case of our brothers in Chechnya who kidnap the Jews in Moscow, and the kidnapping operations in Yemen.

Public Kidnapping: This is when hostages are publicly detained in a known location. The government surrounds the location and conducts negotiations. The authorities often attempt to create diversions and attack the kidnappers. That was the case of the theater in Moscow, and the Russian officers’ detention by Shamil Basayev and the Mujahideen brothers. A counter terrorism officer once said: “There never was a successful kidnapping operation in the world.” This saying was intended to discourage the so-called terrorists. History is full of facts proving the opposite. Many operations by the Mafia, or the Mujahideen were successful. There are examples of many successful operations, such as those of Muhammad’s Army, and Shamil in Moscow. Although not all the goals were met, some of them were. The leader Shamil Basayev’s operation was 100% successful, because it brought the case back to the attention of the international scene, therefore the Mujahideen got their reward, thanks to God.
Stages of Public Kidnapping

- Determining the target: A target must be suitably chosen, to force the government to achieve your goals. Therefore, it is mandatory to make sure the kidnapped individuals are important and influential.
- Gathering enough information on the location (kidnapping stage), and the people inside it. For example:
  - If the people are inside a building: A thorough study of the fences around the building as well as the security and protection teams and systems. A plan of the building with information on its partitions should be reviewed. The kidnappers could use cars that enter the building without inspection to smuggle their equipment. They should also spot individuals who are exempt from inspection when entering the building. When the cars are parked outside the building, the driver could be kidnapped while parking, or the important people when entering with their cars. High places overlooking the building could be set for snipers, and to prevent the enemy from taking advantage of those strategic spots.
  - If the people are on a bus: It is essential to know the nationalities of the people on the bus, as nationalities determine the effect of the operation. All information concerning the bus routing, stops for fuel or rest, protection procedures, the program set for the tourists, and other information should be obtained in order to determine the weak spots, and allow easy control of the group.
  - If the target is on a plane: It is important to determine the destination of the plane. A connecting flight is a better option. Transit areas are more vulnerable where little inspection is provided. Our brothers in Nepal took advantage of such situation, put the weapons on the Indian plane, and hijacked it. Hijackers must be creative in bringing weapons or explosives on a plane. They must also be familiar with the inspection process at airports.
  - If the target is in a convoy: The same rules for assassination in a convoy apply for kidnapping.

Besides specifying the targets, and gathering information on them, leaders must put together a suitable plan made at the level of the weakest team member. It has been said: “A chain is only as strong as its weakest link.”

Execution of the abduction: The abductors’ roles vary, based on the location of the kidnapping operation. They are grouped in three categories: 1) Protection group whose role is to protect the abductors. 2) The guarding and control group whose role is to seize control of the hostages, and get rid of them in case the operation fails. 3) The negotiating group whose role is extremely important and sensitive. In general, the leader of this group is the negotiator. He conveys the Mujahideen’s demands, and must be intelligent, decisive, and determined.

Negotiations: The enemy uses the best negotiator he has, who is normally very sly, and knowledgeable in human psychology. He is capable of planting fear in the abductors’ hearts, in addition to discouraging them. Kidnappers must remain calm at all times, as the enemy negotiator will resort to stalling, in order to give the security forces time to come up with a plan to storm the hostage’s location. The duration of the detention should be minimized to reduce the tension on the abducting team. The longer the detention is, the weaker the willpower of the team is, and the more difficult the control over the hostages is. One of the mistakes that the Red Army made in the Japanese Embassy in Lima, Peru - where they detained a large number of diplomats - was to allow the hostage situation to continue for over a month. In the meantime, the storm team excavated tunnels under the Embassy, and was able to liberate the hostages and end the kidnapping. In case of any stalling, starting to execute hostages is necessary. The authorities must realize the seriousness of the kidnappers, and their dedicated resolve and credibility in future operations.
Hostage Exchange Process: This is a very delicate stage. If the enemy submits to the demands, and the purpose of the operation is to release our imprisoned brothers, it is essential to make sure that the brothers are in good and healthy condition. If the purpose of the kidnapping is to obtain money, you have to ensure that all the money is there, that it is not fake, nor traceable. You must be sure there are no listening or homing devices planting with the money. The brothers must be constantly on alert for possible ambushes. In Bosnia, the UN set up an ambush for the brothers during the exchange; however, the brothers were prepared for it, and prepared a counter-ambush. When the enemy realized that the brother’s readiness and high sense of alert, they let the hostages go without interception. Our Jihadi operations have proven that security forces are not capable of completely seizing control inside the cities. Therefore, the brothers should find ways to transport their liberated brothers even under tight security measures.

Hostage Release: The Brothers should be careful to not release any hostage until they have received their own people. It is essential for the brothers to abide by our religion and keep their word, as it is not allowed for them to kill any hostage after our demands and conditions have been met.

Withdrawal Process: For the withdrawal, some hostages - preferably the most important - must be detained until the brothers have safely withdrawn.

Security measures for public kidnapping

- Detention must not be prolonged.
- In case of stalling, hostages must be gradually executed, so that the enemy knows we are serious.
- When releasing hostages such as women and children, be careful, as they may transfer information that might be helpful to the enemy.
- You must verify that the food transported to the hostages and kidnappers is safe. This is done by making the delivery person and the hostages taste the food before you. It is preferable that an elderly person or a child brings in the food, as food delivery could be done by a covert special forces’ person.
- Beware of the negotiator.
- Stalling by the enemy indicates their intention to storm the location.
- Beware of sudden attacks as they may be trying to create a diversion which could allow them to seize control of the situation.
- Combating teams will use two attacks: a secondary one just to attract attention, and a main attack elsewhere.
- In case your demands have been met, releasing the hostages should be made only in a place that is safe to the hostage takers.
- Watch out for the ventilation or other openings as they could be used to plant surveillance devices through which the number of kidnappers could be counted and gases could be used.
- Do not be emotionally affected by the distress of your captives.
- Abide by Muslim laws as your actions may become a da’wa [call to join Islam].
- Avoid looking at women.

Stages of secret kidnapping

They are very similar to the stages for public kidnapping and include:

- Specifying the target.
• Collecting enough information on the target.
• Setting the plan and providing appropriate training.
• The execution team must be formed of 5 groups:
  o The alarming group that reports the movements of the target;
  o the protection group that protects the kidnappers from any external intervention;
  o the kidnapping group which kidnaps the target and delivers him to a sheltering group;
  o the sheltering group whose role is to keep an eye on the hostage until it is time for exchange or get rid of them;
  o the pursuit deterring group which will ensure the shelter group is not followed or watched.
• Transporting the target to a safe place.
• Getting rid of the target after the demands have been met by transporting him to a safe place out of which he can be freely released. The hostage should not be able to identify the place of his detention.

Security measures for secret kidnapping

Security measures for secret kidnapping include:

• The location where the hostage is transferred to must be safe.
• Beware of the Police patrol.
• While the hostage is being transported, you must beware of Police patrols by identifying their points of presence, to avoid sudden inspection.
• Look for listening or homing devices that VIPs often carry on their watches or with their money. VIPs could have an earpiece microphone that keeps him in touch with his protection detail.
• Everything you take from the enemy must be wrapped in a metal cover and should only be unwrapped in a remote place far from the sheltering group.
• Never make contact from the location where the hostage is detained and never mention him during phone calls.
• Use an appropriate cover to transport the hostage to and from the location. At some point in time the “Allat” party were drugging the hostage and transporting him in an ambulance.
• It is imperative to not allow the hostage to know where he is.
  o In this case, it is preferable to give him an anesthetizing shot or knock him unconscious.

How to deal with hostages in both kidnapping types

• You must check the hostages and take possession of any weapon or listening device.
• Separate the young people from the old, the women and the children. The young people have more strength, hence their ability to resist is high. The security forces must be killed instantly. This prevents others from showing resistance.
• Dealing with the hostages within the lawful control.
• Do not approach the hostages. In case you must, you need to have protection, and keep a minimum distance of one and a half meters from them.
• Speak in a language or dialect other than your own, in order to prevent revealing your identity.
• Cover the hostage’s eyes so that he cannot identify you or any other brothers.
• Wire the perimeter of the hostage location to deny access to the enemy
Endnotes

1 Kim, Wukki, Justin George, and Todd Sandler. Introducing Transnational Terrorist Hostage Event (TTHE) Data Set, 1978 to 2018. Journal of Conflict Resolution, 1-23, 2020, p. 4 (quoted from pre-print version). The authors note: “… hostage-taking attacks constitute only 16.9% of transnational terrorist attacks during 1978-2018. This percentage increased over time as terrorists increasingly resort to kidnappings. Hostage-taking attacks represent the following percentages for three select intervals: 13 %, 1978-1989; 18.1%,1990-2001; and 22.3%, 2002-2018.” The Global Terrorism Database of the START project at the University of Maryland put the percentage of kidnappings as part of all terrorist acts at 15.8 per cent for 2016 - a steep rise from the average of 6.9 per cent for the period 1970-2010. – Cit. UNODC. The Doha Declaration. Promoting a Culture of Lawfulness. Module 16: The Linkage between Organized Crime and Terrorism, p. 1.


4 Kim et al. 2020, p. 16. (quoted from pre-print version). A well-known hostage negotiator commented on these figures as being ‘unreliable’, without, however, being able to offer alternative ones (private communication).

5 Adam Dolnik and Keith Fitzgerald wrote in this regard: “Built on nearly forty years of historical experience, crisis negotiation protocols for managing barricade hostage incidents are well established, and their standard application has, over the years, yielded a staggering 95 per cent success rate.” - Dolnik, Adam and Keith M. Fitzgerald. Negotiating Hostage Crises with the New Terrorists. Westport, Conn.: Praeger Security International, 2008, p. 5.

6 Terrorist researcher who became a hostage negotiator in kidnapping cases. Name withheld by author.


8 Kim et al. 2020.

9 From Kim et al.’s online appendix and replication material. Available at: http://jcr.sagepub.com

10 Kim et al. 2020, p. 20 (quoted from pre-print text).

11 “Kidnapping for Ransom as a Source of Terrorism Funding.” Zürich: ETH, October 2013 (CSS Analysis in Security Policy, No.141). The report noted that in the first half of 2013, “half of the global kidnapping cases were carried out in just four countries: Nigeria (26 per cent), Mexico (10 per cent), Pakistan (9 per cent), and Yemen (7 per cent). Under-reporting of kidnappings is a serious problem. Everard Phillips, writing in 2009, noted.” It is generally accepted within the security and crisis management community that 10% of kidnappings are actually reported; however, Merking and Davis (2001) suggested a conservative self-report figure of 50% of kidnap for ransoms.” - Phillips, Everard, “The Business of Kidnap for Ransom”; in: David Canter (ed.) The Faces of Terrorism. Multidisciplinary Perspectives. Chichester: John Wiley & Sons, 2009, p.191n. – Ann Hagedorn Auerbach wrote in 1998 that “Worldwide the annual kidnap total during the 1990s has been as high as 20,000 to 30,000, counting both political and criminal cases, according to studies by private industry and government groups. By 1997, most experts agreed that the countries most afflicted, starting
with the worst, were: Colombia, Philippines, Brazil, Mexico, Pakistan, Guatemala, the United States, Venezuela, India, and Ecuador.” – Ann Hagedorn Auerbach. Ransom. The Untold History of International Kidnapping. New York: Henry Holt & Co., 1998, p. 23.


14 Regarding the lure of ‘success’, Ann Hagedorn Auerbach noted: “But perhaps the primary factor feeding the crime of kidnapping has been the alluring image of its success. Although only 10 to 30 percent of kidnappings are reported in many countries, the big cases – with big names or big ransom demands – typically are headline news.” Auerbach, Ann Hagedorn, Ransom. The Untold History of International Kidnapping. New York: Henry Holt & Co., 1998, p. 29.

15 Kim, W. et al 2020, p. 16 (quoted from pre-print text).


17 Source: ITERATE data (Mickolus 2006); as quoted in Schmid & P. Flemming 2010, Table 2.5, p. 53.


22 “Colombia. The Terrible Truth”, The Economist, 6 February 2021, p. 34. The report was issued on 28 January 2021 by an institution with the acronym JEP (“special jurisdiction for


24 ITERATE 2006; as quoted in A.P. Schmid & P. Flemming 2010, Table 2.4, p. 52.


31 Ibid.


33 For instance, the official US policy has, until 2015 when President Obama introduced more pragmatic and flexible policies, been one described in these words: “The US Government will make no concessions to individuals or groups holding official or private US citizens hostage. The United States will use every appropriate resource to gain the safe return of US citizens who are held hostage. At the same time, it is US Government policy to deny hostage takers the benefits of ransom, prisoner releases, policy changes, or other acts of concession.”


A RAND study from the 1970s noted that in 66 hostage situations, “Of the total 348 hostages, only 3 per cent were “executed” in cold blood, while 12 per cent died during assaults by security forces.” Brian Michael Jenkins, Janera Johnson, David Ronfeldt, Numbered Lives: Some Statistical Observations From 77 International Hostage Episodes (Santa Monica, CA: RAND Corporation, 1977), p. 27. Available at: http://www.rand.org/pubs/papers/P5905.html

What Brian Jenkins wrote in 1994 is still largely true: “There are no reliable international statistics on kidnappings. Fear of retribution, incompetent or corrupt police, or laws that prohibit the payment of ransom, provide powerful disincentives to reporting an abduction, and governments themselves, seeking foreign investment or tourism, have little incentive to broadcast a kidnapping problem. As a result, there may be great disparities between official statistics and informed estimates. The numbers are useful only in identifying high-risk areas and spotting long-term trends.” – Cit. Ann Hagedorn Auerbach 1998, p.23.
Ann Hagedorn Auerbach arrived in her study from 1998 at similar figures regarding survival rates, citing “One five-year study, beginning in 1992, showed that of the foreign nationals kidnapped, 66 percent were eventually released after some sort of negotiation, 20 percent were rescued, 9 percent were killed or died in captivity, and 5 percent escaped. Roughly half of the captives were held from 1 to 10 days, a quarter were held from 11 to 50 days, and the rest from 50 to over 100 days.” Ann Hagedorn Auerbach. Ransom. The Untold History of International Kidnapping. New York: Henry Holt & Co., 1998, p. 35.

This was, for instance, the case in Chechnya in the 1990s. One analyst reported: “…between January 1997 and August 1999, 1,094 civilians were kidnapped for ransom, the average settlement ranged from $5,000 to $145,000 per hostage. The income was used for purchasing weapons and modern armaments during the conflict, and was also reinvested to fund further kidnappings so as to maintain the business.” Phillips, Everard, “The Business of Kidnap for Ransom”; in: David Canter (ed.) The Faces of Terrorism. Multidisciplinary Perspectives. Chichester: John Wiley & Sons, 2009, p. 201. (The analyst Phillips referred to is Makhuna, author of: I. Makhuna (2005): “Islamic terrorism and the question of national liberation, or problems of contemporary Chechen terrorism.” Studies in Conflict & Terrorism, 28, pp. 515-532). See also: Ann Hagedorn Auerbach 1998, p. 23.


Bibliography


With many thanks to Judith Tinnes from whose larger unpublished bibliography many of these titles were taken.


Web-based Resources


Loertscher, Seth, (2020) ‘Combatting Terrorism Center at West Point’. Available at: https://ctc.usma.edu/view-ct-foxhole-rob-saale-former-director-u-s-hostage-recovery-fusion-cell/


US Department of State, Overseas Security Advisory Council. *Kidnapping: The Basics*. Washington, DC: OSAC. Available at: https://www.osac.gov/Content/DownloadAttachment?contentType=Report&contentItemId=ec9e4092-cbf6-4fb7-b301-15f4ae161d01&contentItemAttachmentId=40
Suicide attacks have been a feared tactic of terrorism since the initiation of suicide bombings in Lebanon in the 1980s, and perhaps even more so since their adaptation in the airplane attacks on the United States on 11 September 2001 (9/11). Numbers of suicide attacks, especially suicide bombings, have increased over time, in some cases dramatically, and there is a clear public interest in understanding how these types of attacks may be prevented. Is it possible to prevent suicide attacks by terrorists, and, if so, by what means? In fact, there are examples of effective efforts to prevent suicide attacks. One example involves the prevention of suicide bombings in one context – Israel. Suicide bombings peaked in Israel in 2002 and 2003, but decreased between 2003 and 2005. One explanation for this decrease is effective counterinsurgency (COIN) and counterterrorism efforts implemented during and following the Second Palestinian Intifada. Terrorism has continued – even increased – in Israel, but suicide attacks are no longer a common occurrence. Another example involves the prevention of one type of suicide attack – attacks using commercial airplanes. Changes in airport and airplane security after 9/11 have made it harder for terrorists to target or utilize airplanes in attacks. Counterterrorism efforts have not stopped terrorists from attempting further attacks on airports and airplanes, yet these attempts have been met with additional hardening of these targets. While counterterrorism efforts in Israel and against attacks on airplanes have been largely successful, these successes have not included remedies for the sources of the violence that inspire groups to use suicide attacks or individuals to participate in them. The groups responsible for the suicide attacks in Israel and on 9/11 continue to operate and continue to support violence.

Keywords: COIN, counterterrorism, suicide attack, suicide bombing, strategy, terrorism, terrorist tactics.
There is clear public interest in preventing suicide terrorism. The people who carry out suicide attacks act like guided missiles with the capacity to identify times and places to strike in order to maximize the terror of their attacks. Suicide attacks often cause more destruction, kill more people, and gain more attention than non-suicide attacks. Threats of these attacks perpetuate fear within larger communities and raise the coercive capacity of otherwise weak non-state actors.

Suicide terrorists often target civilians in places of perceived safety, outside an active conflict zone. No single event illustrates the devastation of suicide attacks more plainly than the 9/11 attacks in New York, Washington DC, and Pennsylvania. The tremendous loss of life, destruction, and disruption associated with these attacks showed the potential for similar attacks in the future, guided by unknown adversaries capable of directing and inspiring attacks from faraway places. The surprise of the attacks, along with the attackers’ choice of weapons, targets, and scale, drew new attention to an otherwise well-established tactic of terrorism. While the 9/11 attacks marked a change in the awareness given to this specific modus operandi, they did not mark the beginning of the study of suicide attacks, their causes, or ways to prevent them.

Suicide attacks were not a new tactic brought into the twenty-first century by groups like al Qaeda. They were a tactic introduced in the form of suicide bombings twenty years earlier in Lebanon during the country’s fifteen-year civil war – though their origins are much older.  
Since that time, suicide bombings evolved from what was initially an insurgent tactic used primarily against government and military targets in the context of civil war into a tactic of terrorism aimed at civilians in times of relative peace. Suicide attacks increased in frequency after 2001, despite enhanced counterterrorism efforts, and in some cases perhaps as a side-effect of these efforts or in response to them.

At the same time, and notwithstanding the increase in the number of attacks overall, there is some evidence of success in preventing suicide attacks by terrorists, and lessons can be learned from these examples. One example is what appears to be the successful prevention of a repeat of the 9/11 attacks, during which civilian airplanes were used as guided missiles. A second example is the decrease in suicide bombing in Israel during and after the Second Palestinian Intifada.

The focus of this chapter is on prevention. Is it possible to prevent suicide attacks by terrorists, and, if so, by what means? This is not a question about preventing terrorism, in general. Rather, the focus is on preventing one type of attack, specifically suicide attacks, carried out by a specific type of non-state actor, namely a group that engages in terrorism.

Answering these questions requires attention to the role of suicide attacks in terrorist strategy, patterns in the adoption and innovation of terrorist tactics, and the seemingly open-ended threat of future terrorist violence. It also requires attention to past efforts to prevent terrorist attacks, including successful counterterrorism efforts aimed at dwarfing specific types of attacks, as well as cases in which suicide attacks have been effectively halted.

The discussion begins with an outline of what it means to refer to suicide attacks by terrorist groups. The second section includes a discussion of early suicide bombers and the evolution of suicide attacks. The third section consists of analyses of two examples of successful prevention of suicide attacks by terrorists. The first example focuses on changes in air travel after 9/11, including a description of how one type of suicide attack has been prevented. The second example focuses on Israeli counterinsurgency (COIN) and counterterrorism, including a description of how one state significantly reduced the frequency of suicide bombings within its borders. This discussion is followed by explanations of alternative reasons for a decrease in suicide bombings. The final section includes considerations of implications and limitations.
Distinguishing Terrorism and Suicide Attacks

Terrorism is a type of political violence perpetrated primarily against civilian or noncombatant targets with the goal of provoking widespread fear as a means of bringing about a desired political change.\(^3\) Terrorist groups are political groups, understood as groups motivated by political objectives, that use terrorism as a tactic in pursuit of their goals. The terrorism label belongs to individuals as well as those working within a terrorist group or network, including perpetrators of attacks, those who plan and orchestrate attacks, others who act in supporting roles, and their leaders. To some extent, terrorists share, regardless of role, an expectation that attacking and generating fear among civilians or noncombatants will help them achieve their goals.\(^4\)

Terrorist groups do more than engage in acts of terrorism.\(^5\) The same groups that attack noncombatants and civilians may also attack military and hardened government targets, and they may do so in peacetime or in the context of war, at home or abroad. Attacks on “softer” civilian targets are prototypical terrorist attacks. Attacks on “harder” armed targets are not necessarily terrorism, even though the perpetrators may be terrorists. Attacks on “harder” state targets tend to require more capable and better-trained militants. Some terrorist groups have these capabilities, and those that do may be more appropriately identified as insurgents, especially if terrorist attacks are not their dominant form of attack.\(^6\)

It is no coincidence that the groups labeled as terrorists by some experts are labeled as insurgents by others. There is considerable overlap between these labels. Insurgents are political actors seeking to change a political system, such as by installing a new regime or establishing a new state. Their adversaries are states and other non-state actors, and their tactics often include a combination of terrorist attacks and guerrilla warfare techniques.\(^7\) Although insurgencies are generally associated with sustained conflict or larger-scale warfare, this is not always the case.\(^8\) The weakest (would-be) insurgents may fail to create and sustain the level of violence or disruption typically associated with a protracted “insurgency.”\(^9\)

Insurgents’ combination of guerrilla operations and terrorist tactics depends to some extent on their strength. Some insurgents control territory. Those that do, tend to have more resources and operate more openly. They may collect “taxes” to fund their operations, and they may develop a trained and possibly even a uniformed militia.\(^10\) Weak insurgenst may be relegated to carrying out attacks on “softer” unarmed targets, essentially relying on terrorism, while stronger insurgents are capable of attacking “harder” armed targets, typically with guerrilla tactics, such as sabotage, ambushes and hit-and-run attacks. They rarely have the capacity to engage in direct military confrontation. The insurgents using guerrilla tactics are guerrillas. The insurgents using terrorism are terrorists. Insurgent groups are often both guerrilla and terrorist.

Suicide attacks are one tool used by a subset of insurgents for guerrilla and terrorist attacks. Suicide attacks are a type of attack for which the death of the attacker is necessary for the successful completion of the attack.\(^11\) This is a “narrow,” or “strict,” definition of suicide attack, as compared to definitions that require only a high likelihood of an attacker’s death for a mission’s success.\(^12\) Even when the attackers’ deaths are highly likely, their deaths may not be required for an attack to be successful. Perpetrators of gun and knife attacks have a high likelihood of being killed while carrying out an attack, but their deaths are not a requirement for their attacks to be successful, and there is a chance of survival. Suicide bombings are attacks that practically guarantee the death of the perpetrator. Suicide bombers expect to die when they detonate their explosives. That suicide bombers are willing to die, and are consenting to die, is a necessary element of a narrow definition of the phenomenon.\(^13\) It is also a condition that is impossible to ascertain in many cases. For example, some “suicide bombers” are themselves victims, who have been kidnapped or coerced before being armed with explosives they cannot remove. There are also cases of remote detonation of “suicide” bombs. Attacks that do not require the death of a perpetrator or do not have a willing perpetrator are not suicide attacks.
according to the strict definition, yet they may be counted as such given the limited information often available.

Suicide attacks are terrorism when the primary targets of the attacks are civilians or noncombatants and the intent of the attacks is to spread fear in order to bring about a desired political advantage or change. The same group may use suicide attacks against “softer” civilian targets as well as against “harder” government and military targets. As such, a single group may carry out suicide attacks that qualify as terrorism as well as suicide attacks that are more consistent with guerrilla warfare. References to suicide attacks by terrorist groups, which are the focus of this chapter, include the subset of attacks that are aimed at military and government targets, so long as the perpetrators of these attacks are non-state actors that also target civilians in terrorist attacks.

Early Suicide Bombers

Suicide bombing began spreading as a terrorist and insurgent tactic in the late twentieth century. The first suicide bombings by terrorists gained attention in the early 1980s, during Lebanon’s fifteen-year sectarian civil war (1975-1990). Lebanon’s early suicide bombers drove explosive-laden vehicles into their targets, most of which were military and state targets. Some of the militants using suicide bombings were reportedly (co-)sponsored by Iran and Syria, and their targets were also adversaries of these states.

One of the roots of suicide bombing as a tactic of terrorism may be traced to Iran and Iranian propaganda from the era of the Iran-Iraq War (1980-1988). During the war, the newly established Islamic Republic of Iran encouraged its soldiers, including untrained youth volunteers, to embrace self-sacrifice in the protection of the state. Propaganda celebrating the sacrifice of a thirteen-year-old child soldier offers one example. As the story has been told, the child detonated grenades in front of an Iraqi tank, halting its progress and saving many civilian lives in the process. The story provided support for an official narrative, which drew connections between self-sacrifice for the state and for the larger Shia community, with promises of rewards in the afterlife. While the Iran-Iraq War continued, violent political groups, including some with ties to Iran, were among the first to carry out suicide bombings – often termed martyrdom operations – in Lebanon.

Most suicide bombings in Lebanon, including those attributed to Lebanon’s Hezbollah, targeted harder, non-civilian targets. In the context of civil war, many of these bombings could – if they targeted military objects – be considered as acts of war by weak insurgents rather than as terrorist attacks. Iraq’s embassy was the first target of suicide bombers in Beirut in 1981, while Iraq was at war with Iran. Suicide bombers attacked the US embassy in Beirut twice, in 1983 and 1984. Simultaneous suicide bombings in 1983 targeted the barracks of American marines (killing 241) and French paratroopers (killing 58) in different parts of Beirut. Suicide bombers attacked Israel’s military in southern Lebanon on multiple occasions. The civil war’s deadliest suicide bombings targeted foreigners.

Hezbollah has received attention as the initiator of suicide bombings. The group may not have carried out the first suicide bombing, and it was not the most prolific user of suicide attacks, yet the group inspired other groups to copy its suicide bombing tactics for use in their own conflicts. In Lebanon, suicide bombings ceased for a time with the end of the civil war in 1990. Hezbollah and other militant groups turned to party politics, participating in Lebanon’s post-war power-sharing governments. Lebanon’s militant groups remained active during this time, with many of the attacks in the country credited to Hezbollah. Suicide attacks, however, were far less common. As the frequencies of suicide bombings declined in Lebanon, they were increasing elsewhere.

The Liberation Tigers of Tamil Eelam (LTTE or Tamil Tigers) adopted suicide tactics in the late 1980s. The Tamil Tigers were nationalist-separatist insurgents engaging in what would
become a decades long civil war in Sri Lanka. Unlike Hezbollah, the LTTE was a secular group with a membership that was primarily Hindu and Christian. The Tamil Tigers had observed the apparent success of suicide bombings in Lebanon and reportedly went so far as to obtain training from Hezbollah on how to use these tactics in their insurgency. The Tamil Tigers also added their own innovation, the suicide vest or belt, such as the one used in the May 1991 assassination of former Indian Prime Minister Rajiv Gandhi. Until the American-led 2003 invasion of Iraq, when suicide bombings surfaced there, the secular Tamil Tigers had carried out more suicide attacks than any other group.

The Tamil Tigers were relatively strong by insurgent terms. They organized themselves as military units, with specialized forces, including an army, a navy, and the beginnings of an air force, known as the Tigers, Sea Tigers, and Air Tigers, respectively. The Tamil Tigers employed a special operations force devoted to carrying out suicide attacks, which was known as the Black Tigers. The Sea Tigers also became a “suicide force,” referred to as the “Black Sea Tigers.” As with the insurgents in Lebanon, most of the Tamil Tigers’ suicide attacks were aimed at military, police, and government entities.

Palestinian militants adopted suicide bombings in the 1990s, taking lessons from Hezbollah’s vehicle-borne bombs and the Tamil Tigers’ suicide bomb vests. Secular Palestinian groups had had strongholds in Lebanon prior to being expelled during Lebanon’s civil war. Hezbollah and the Palestinians were at odds during that time. After the civil war, however, they again viewed Israel as their main adversary. Moreover, the first Palestinian suicide attackers were members of a different Palestinian political group. They were not the exiled members of the Palestinian Liberation Organization (PLO); rather, they came from the religious nationalist groups that formed during the PLO’s absence. Members of the Islamic Resistance Movement, better known by the acronym Hamas, were deported to Lebanon in 1992, where they became acquainted with Hezbollah and its tactics.

Unlike in Lebanon and Sri Lanka, civilians were the primary targets of Palestinian suicide attacks in Israel and in the Palestinian territories. These were terrorist attacks. Also unlike in Lebanon and Sri Lanka, militants initiated suicide attacks at a time of relative peace. Suicide bombings began during and following the Israeli-Palestinian peace negotiations in Oslo, Norway. The negotiations, which resulted in the Oslo Accords, included representatives of Israel and the PLO. Hamas, which was among the groups opposed to peace negotiations and excluded from the new, nondemocratic Palestinian Authority (PA) government, was the first group to carry out a suicide bombing in Israel. In fact, Hamas’ violent opposition made the group a target of counterterrorism operations undertaken by Israel and the post-Oslo Accord PLO-led PA government. The same was true of other opposition groups, such as the Palestinian Islamic Jihad (PIJ), which were weakened by the peace and weak by comparison to their PA counterparts.

Suicide attacks spread further, beyond Israel and the Levant. The secular Kurdish Workers’ Party (PKK) adopted suicide bombing tactics, followed by al Qaeda, Chechen militants, and the Taliban. The tactics appealed to groups from Egypt, India, Indonesia, and the Philippines, among others. Al Qaeda’s new affiliates used suicide tactics after 2001. Boko Haram began using suicide tactics nearly a decade later. The most prolific users of suicide attacks since 2003 operate in Afghanistan, Iraq, Nigeria, and Pakistan. There were more suicide bombings in Iraq within a few years of the 2003 invasion and occupation than there had been worldwide since the initiation of suicide bombings in Lebanon.

There are many reasons for the spread of suicide terrorism. As those targeted by the early bombings would soon realize, insurgents had found a way to exploit security vulnerabilities. Suicide bombings appeared to work, at least in the sense of achieving some of a group’s objectives. Several foreign powers abandoned their positions in Lebanon after suicide bombers targeted their embassies and military installations. American and French forces
withdrew from the country in 1984. Israeli forces remained in southern Lebanon but withdrew in 1985 to a “security zone” along Lebanon’s southern border.\(^{35}\)

Another reason for the spread of suicide attacks is that militants innovate. They adopt new tactics and adapt them to their operations. Suicide bombings gave weaker groups new opportunities. They could reach “harder” targets with greater effect. The early weapons, often in the form of suicide truck bombs, could blend into regular traffic. Vehicles can hold large amounts of explosives and their drivers could force their way into places militants ordinarily could not reach. Insurgents and terrorists who adopted suicide bombing tactics, including those outside Lebanon, found different ways of transporting explosives and improvising explosions, new carriers for their explosives (including women and children),\(^{36}\) and new targets.

Once adopted, suicide bombings may become part of a group’s *modus operandi*. The reasons some terrorist groups continue carrying out suicide attacks differ from the reasons they adopted these tactics in the first place. After a group invests in the infrastructure and expertise needed to carry out suicide attacks, these tactics become part of the way they “do business.” Moreover, since most militant groups generally have limited capacities,\(^{37}\) investing in one tactic (such as suicide bombings) means diverting resources from other types of operations. Suicide tactics become one of the tools militants may use, but they may also replace other tools.

The initial spread of suicide tactics may have reinforced further spread, as such attacks began to be seen as acceptable among a subset of extremist militant groups. With their spread, suicide attacks became what can be called the “emblematic deed” of the latest “wave” of terrorism.\(^{38}\) For many insurgents, suicide attacks became their “most sophisticated tactic,” with suicide attackers acting as guidance systems for powerful explosives in attempts to maximize the impact of their attacks, as well as the “psychological effect” these attacks would have on their targets.\(^{39}\)

While many of the groups using suicide attacks remain active, patterns in the use of these tactics among the earliest adopters provide some insight into the conditions under which suicide attacks may decline or cease. In Lebanon, some groups that used suicide attacks became involved in government. They were not defeated; rather, they were incorporated into the political system. Terrorism in the form of assassinations continued, yet there were far fewer suicide bombings. Suicide bombings returned to Lebanon in 2006 with different perpetrators, notably al-Qaeda affiliates and the Islamic State. Ironically, the targets of suicide attacks included Hezbollah, the party credited with initiating and spreading suicide tactics a quarter-century earlier. Suicide attacks ended in Sri Lanka in 2009 with the death of the Tamil Tigers’ leader, the defeat of the insurgent group, and, as in Lebanon, the end of the civil war.\(^{40}\)

The decrease in suicide attacks in Israel differs in important ways from the experiences in Lebanon and Sri Lanka. As in Lebanon and Sri Lanka, the sharp decrease in suicide attacks coincided with the end of violent conflict. The groups perpetrating the attacks against Israel, including Hamas, PIJ, and militants affiliated with Fatah and others, survived the Intifada and have continued their opposition to Israel and each other. A key difference is that they no longer carry out as many suicide bombings as they once did.

There are reasons to believe that the Second (al-Aqsa) Intifada (2000-2005) ended at least in part because the Palestinian groups were no longer able to carry out their deadliest attacks, including suicide bombings. As such, it may not be that suicide attacks ended because the Intifada ended, but rather the reverse. The Intifada ended because the groups could no longer physically reach their desired targets. Effective COIN and ongoing counterterrorism operations by Israel weakened the groups’ capacity to carry out suicide attacks, even while their desire to attack remained intact. In this way, Israel’s COIN and counterterrorism efforts offer a unique case. Israel achieved a significant decrease in the threat of suicide terrorism without defeating the groups responsible for the attacks, and without removing the threat of violent resistance. Israel faces an ongoing threat of terrorism, but no longer a significant threat of suicide terrorism.
Israel offers one case of suicide terrorism prevention that deserves further consideration. Another case worth discussing involves the efforts to prevent a repeat of a 9/11-style attack from the air. The Israeli case shows this application to a context, or place, in which suicide attacks decreased. The post-9/11 case suggests successful prevention of a specific type of attack, though not an attack tied to a place. Both examples involved a combination of COIN and counterterrorism responses, and both reductions are likely the result of the counterterrorism efforts.

Preventing Suicide Attacks on Passenger Planes

Preventing suicide attacks is distinct from preventing terrorism in general. There seems to be consensus among counterterrorism professionals that terrorism, as a tactic, will not disappear. Some of the ideologies associated with terrorism change over time, together with weapons and tactics. Yet the practice of targeting civilians remains a constant feature of this type of political violence. Terrorists may be defeated, but terrorism as a coercive tactic will continue and new terrorist networks will emerge. One of the reasons behind a change in tactics has to do with the introduction of new technologies, relating to instruments and targets of attack. Another reason that terrorist tactics change is the fact that targets become more resilient, meaning that certain targets become hardened to prevent at least some types of attacks. Air travel is a useful example of a new technology and a new target, which has been hardened repeatedly in response to new threats.

The expansion of international air travel in the mid-twentieth century created new opportunities for terrorists. Airplanes and their passengers became valuable civilian targets, which terrorists could direct to their desired locations and exchange for specific concessions. For a time, skyjackings were the “spectacular attacks” that gained widespread media attention. In-flight bombings of airplanes were less common but even more terrifying. Whereas hostages could survive their ordeals, plane bombings were often more lethal.

The era of skyjackings and plane bombings came to an end, for the most part, with changes in airport security. Metal detectors made it difficult for hijackers to board planes with the types of weapons they would presumably need to commandeer an aircraft and control its passengers. Scans of luggage made it more difficult for terrorists to load explosives onto planes. Assurances that passengers traveled with their luggage may have deterred plane bombings at a time before groups began employing suicide attackers. Additional barriers at airports included allowing only ticketed passengers to approach gates for international flights. Airplane hijackings and bombings decreased in number as airport security increased and airplanes became harder targets. However, these efforts did not stop terrorism, and terrorists found new ways to carry out attacks.

In the 1980s and 1990s, suicide bombings began to replace skyjackings as the new “spectacular” type of attack. Suicide bombings allowed militants to perpetrate devastating attacks and gain enormous media attention in the process. Much of the attention related to the ways these attackers could maximize their impact in terms of death, destruction, and disruption, as well as to the types of targets they could reach. Questions regarding how to deter attackers who are willing to kill themselves while killing others also gained attention.

The 9/11 attacks represented a further innovation. The attackers took advantage of remaining vulnerabilities in air travel with a combination of skyjacking and suicide bombing. Unlike the hijackers of earlier decades, the 9/11 hijackers were on suicide missions. Also unlike their predecessors who carried explosives in vehicles, belts, or vests, the 9/11 hijackers did not require explosives or other traditional weapons. The 9/11 attackers also differed from some of their predecessors in that they were educated, privileged, and well-traveled. They could board the planes without drawing attention. They could commandeer aircraft and kill thousands
of people without possessing a gun (just knives and mace or pepper spray). They used airplanes as weapons.

The absence of a repeat of the 9/11 attacks nearly twenty years later suggests a measure of success in counterterrorism efforts. Air travel has become an even “harder” target and tool for terrorists. Airport and airplane security continue to change in response to new and potential threats. New types of scans, enhanced background and identification screenings, additional restrictions accessing departure gates, and no-fly lists have further hardened air travel. Changes in airplane security have included reinforced cockpit doors, restrictions on congregating near the cockpit, restrictions of carry-on items, and embedded law enforcement (air marshals), along with training of airplane staff and, in some cases, vigilant passengers. Furthermore, the possibility that fighter jets would intervene in future attacks diminishes what attackers might hope to achieve even if they could take control of a plane.

This is not to suggest that there have not been further attempted and successful suicide attacks involving aircraft since 9/11. There have been a few, but they have had little success. Attempted suicide attacks on commercial airplanes, including the “shoe bomber” and the “underwear bomber,” have been followed by further hardening of airplane and airport security.

At the same time, the hardening of airplanes and access to passenger planes is only part of the story. Attacks like the ones on 9/11 require more resources and know-how than most terrorist groups can muster. It was already difficult for the planners of the 9/11 attacks to find 19 people who were capable and willing to carry out the attacks.46 It has likely become even more difficult to find attackers for such missions given increasing security in air travel.

Instead of targeting airplanes, however, terrorists have found targets in other modes of transportation. On 7 July 2005, suicide attackers targeted London’s transportation system. One of the best defenses from attacks such as these, beyond effective counterterrorism, may be widespread disdain for these types of attacks and the groups responsible for them.

Preventing Suicide Bombings in Israel

Israel’s operations during and after the Second Palestinian Intifada offer another example of COIN and counterterrorism efforts, which were followed by a sharp reduction in suicide bombings. Palestinian militants began using suicide bombings in Israel and the Palestinian territories in 1993, toward the end of the First Palestinian Intifada (which began in 1987). Their first targets were Israeli civilians traveling on busses. Subsequent targets included restaurants, clubs, markets, and other places where civilians gathered. Suicide bombings continued throughout the 1990s. By one estimate, more Israelis died from acts of terrorism between 1993 and 1998 than during the previous fifteen years.47 The early years stand in contrast, however, to the intensification in suicide bombings that began in 2001 and peaked in 2002. After that, suicide bombings began to decrease in number in 2003 and 2004. They became rare occurrences by 2005. What led to this decrease? Moreover, if the decrease was a response to effective COIN and counterterrorism, which operations contributed to this outcome?

In the case of Israel, the answer appears to be that efforts aimed at weakening militants and hindering their ability to coordinate and access targets were effective in raising the costs and restricting opportunities to carry out suicide attacks, leading to an overall reduction in the number of such attacks.48 While Israel’s approach to countering suicide terrorism may not be separated from the state’s approach to countering terrorism, more generally, it is the significant decrease in the number of suicide attacks that stands out.

The story of the prevention of suicide attacks in Israel requires an overview of the initiation of suicide attacks against Israeli targets and an explanation of the sources of Israel’s increasing vulnerabilities in the years leading to the Second Intifada. It is useful to divide Israel’s experience with suicide terrorism into three periods. The first period began in the early 1980s during Israel’s intervention in Lebanon. The targets of these bombings were military, and the
attacks took place in the context of war and occupation. The second period began in 1993, with suicide bombings aimed at civilians in Israel. These bombings preceded the completion of the peace negotiations in Oslo. This period is important because it was during this time that Israeli counterterrorism efforts were severely reduced. In effect, the peace process helped to establish the conditions under which suicide attacks would increase. The third period corresponds to the Second Palestinian Intifada, which began in 2000. Between 2000 and 2004, Israel rebuilt its capacity to counter Palestinian militancy. It was also during this time that suicide bombings peaked and later subsided. Israel’s counterterrorism measures were successful in the short run, leading to a decrease in Palestinian militancy. More importantly, these efforts were successful in the long run in terms of reducing suicide bombings. Israel’s counterterrorism approach stands out for this success.

**First Period: Lebanon in the 1980s**

Israel became a target of suicide bombings in Lebanon in the early 1980s. The context was Lebanon’s civil war. Israel’s initial invasion of Lebanon concentrated on southern parts of the country. The PLO, an umbrella organization dominated by Yasser Arafat’s Fatah, sought to establish an autonomous “Fatahland” in this part of Lebanon, and Palestinian militants used this territory as a base for launching attacks on Israel. Palestinian militancy threatened Lebanon’s sovereignty, including control over its southern territories, while Palestinian terrorism invited violent reprisals from Israel.

Israel’s invasion of Lebanon led to greater involvement in the civil war. Israel allied with Lebanon’s Christian militias, including the Phalangists. The Christian militias were Israel’s “natural allies” in Lebanon. The Christians were the largest of Lebanon’s communities. They were also the least opposed to Israel, and they had common adversaries. A Palestinian attack on the Phalangist leader, a leader within the Christian community, had been a spark for the civil war. Yet, the Christian militias were also weak and divided.

The PLO was pushed out of Lebanon in 1982, midway through the civil war, but Israel’s adversaries in Lebanon had expanded to include Shia militants. Hezbollah, which appeared in 1982, was one of these adversaries. It is also the group that later became known for weaponizing suicide tactics. Hezbollah began using suicide bombings against Israel’s military while the Palestinian militants, most of whom were Sunni, were not yet turning to suicide tactics.

These first suicide bombings were not aimed at civilians. Suicide bombers struck Israeli forces and pro-Israeli militias between 1982 and 1986. In mid-1985, Israel withdrew from much of Lebanon, though it maintained a presence in a smaller strip of Lebanese territory along the states’ shared border. Suicide bombings against Israeli targets ceased for several years after Israel’s withdrawal to this security zone. This happened even before the end of Lebanon’s civil war, before Hezbollah’s transition to a political party participating in government, and a decade before Israel withdrew completely from Lebanon’s southernmost territory.


As the war in Lebanon came to an end, Israel faced new challenges combatting terrorism at home. This soon included suicide terrorism. The First Palestinian Intifada had begun in 1987 as a popular protest movement, led by local Palestinians independent of the exiled PLO leadership. Suicide bombings were not part of this intifada, nor were they tactics previously used in this context.

In 1993, Israel negotiated a transitional arrangement with Yassar Arafat’s PLO as the representative of the Palestinian people. This was an important move for the PLO, as the group
had been in exile, away from its people and at risk of becoming increasingly irrelevant among younger Palestinians. Meanwhile, the group’s political competitors, including Hamas, had gained popular support in the PLO’s absence. The talks culminated in the signing of the Declaration of Principles on Interim Self-Government Arrangements. This agreement set forth goals and guidelines for a peaceful transfer of power over governance and a measure of autonomy for Palestinians. The agreement would allow the PLO to return from exile, assume control of a transitional Palestinian government (the Palestinian Authority, PA), prepare for eventual democratic elections, and “strive to live in peaceful coexistence.”

There were also several immediate problems.

In terms of establishing self-governance, the Palestinians began at a disadvantage. The Palestinian Authority (PA) did not have a state to govern. The Declaration had not established a Palestinian state, or even an entity that could become a state. The Palestinian-controlled areas of the West Bank were noncontiguous, a collection of cities and towns connected by roads and surrounded by Israeli territory. Israel reserved land and controlled settlements within the territories. The Gaza Strip was already separated from the West Bank by a span of Israeli territory, as it had been for more than four decades, and it was a stronghold for the PLO’s opposition. The prospects were not good for the new PA.

On top of this, the PLO was weak. The organization had gained legitimacy as a negotiating partner, signatory to the Declaration, and organizer of the transition to a form of autonomy within the Palestinian territories. At the same time, the initial Palestinian leadership was not chosen by the people, nor was the agreement it reached with Israel universally accepted by its local competitors. The organization was disconnected from the Palestinian people and its top leaders had not resided in the Palestinian territories for some time. The organization also suffered from perceptions of corruption and enrichment at the expense of the Palestinian people.

Another disadvantage for the Palestinians was their lack of experience with governance. The PLO had prior experience with some types of administration, such as supporting schools and social projects, but with other aspects of state building it was less familiar. In addition, the PLO had no practical experience, and possibly little real interest, in the democracy for which the Declaration called.

Following the Declaration, the new PLO-led PA set about creating a police force, which would be responsible for maintaining law and order within the areas under Palestinian control. Palestinians were charged with policing other Palestinians. The PLO employed former militants in its new police forces and in other security roles. Militants were trained and armed, and their numbers swelled beyond the initial prescription. In addition to being larger, the security apparatus was also given a more expansive protocol than originally intended. This included offensive capabilities. The new security forces included military intelligence, military police, and paramilitary forces. Former terrorists became counterterrorism agents. This meant that Palestinians, including former militants, would investigate Palestinian “terrorists” alongside Israeli counterterrorism forces. The forces were armed, trained, and tasked with policing themselves and their political opponents. They were given access to information regarding security threats, some of which originated with groups and individuals opposed to the PLO. At the same time, the PLO lacked incentives to police itself. The organization prepared for a potential renegotiation of the interim agreement. One fear was that the new Palestinian forces, as a collection of armed groups, would be capable of projecting force against Israel, a concern that was shown to be legitimate during the Second Intifada. This was the backdrop for the initiation and eventual escalation of suicide bombings against Israeli civilians.

Adding to this, the new state of affairs in the Palestinian territories did not eliminate opposition to the PLO or to the agreement the PLO had made with Israel. Among the opponents were parties that had been excluded from the negotiations as they had disagreed with the very nature of the transitional peace. The PLO’s more religiously oriented and less compromising
local competitors, Hamas and PIJ, were among them. Both groups opposed recognizing Israel through negotiations and opposed anything short of full Palestinian statehood. They were not supportive of the new Palestinian leadership or the compromise, which gave the PLO power. As opposition parties, they threatened the PLO’s dominance. Because they continued to use terrorism, they positioned themselves as “spoilers” and as targets of the Palestinian police and Israeli counterterrorism forces.

The agreement was not ideal for Israel either. Israel gained a weak, though empowered, neighbor and counterterrorism partner. The Declaration called for Israel to vacate the Gaza Strip and Palestinian cities within the West Bank. Israel withdrew from the Gaza Strip and withdrew its military and relinquished power over policing in much of the West Bank. While Israel could retain control over some sources of intelligence, including visual and signal intelligence, the military withdrawal meant a loss of valuable human intelligence.

These losses were disastrous for Israel’s counterterrorism efforts. Although Israel retained authority over counterterrorism and border security, Israel no longer had access to the human intelligence upon which the state had relied. Israel lost access to local informants, those who previously had provided crucial information on potential threats. Information gathered through signal interceptions, such as through radio transmissions and over the internet, were less useful without the context provided by informants on the ground. Israel also lost access to the Palestinian communities from which terrorist threats emerged. These were communities that it could previously police. The result was a sharp reduction in information on Palestinian militants, operations, and, hence, potential threats. When Israel withdrew its military from the Gaza Strip in 1994, it lost access to the territory dominated by Hamas and PIJ, which could operate at a distance even from the PLO and the new PA in the West Bank.

While the PLO was occupied with establishing the basis for a future government and building police and other forces, its competitors continued “sabotaging the peace.” The attacks leading up to the Second Intifada demonstrated that the PLO could not negotiate peace for all Palestinians and could not guarantee the peace to which it had agreed.

Suicide bombings were a new tactic in the hands of Palestinians. While Israel’s military had experience with suicide bombings in Lebanon, these had not been introduced within Israel, nor had these been used against Israeli civilians. The perpetrators were not from the PLO or Fatah, which took the lead in peace talks and governance; rather, the perpetrators were their political opponents, groups that were excluded from the talks. Hamas took credit for the first of these attacks. PIJ soon joined in carrying out suicide bombings.

Hamas’ first suicide bombing was in April 1993 in the West Bank. The targets were a civilian bus and a military bus. There was another suicide car bombing six months later in October 1993, this one aimed at a bus near a military site in Beit El, also in the West Bank. The timing of the first suicide bombing coincided with progress in the Oslo peace negotiations. The second successful attack followed shortly after the signing of the Declaration.

More suicide bombings followed between 1994 and 2000. The yearly number of suicide bombings remained in the single digits each year through 2000. Civilians were the frequent targets of suicide attacks, and attacks on buses and gathering places were more frequent and associated with more casualties than attacks on military or police. Hamas and PIJ were the main perpetrators during this period.

**Third Period: Second Palestinian Intifada 2000-2004**

A dramatic increase in the number of terrorist attacks, including suicide attacks, followed the onset of the Second Palestinian Intifada in December 2000. Suicide bombings peaked in 2002, with most of these bombings taking place in Israeli towns and cities, and most of those targeted being noncombatants. March 2002 was the deadliest month in terms of suicide bombings.
The Second Palestinian Intifada differed from the First and from the interim “peace” in that terrorism, including high-casualty suicide attacks, became a more frequent occurrence. At the height of the new Intifada, suicide bombings were a big part of this threat. In previous rounds of the Israeli-Palestinian conflict, Palestinian deaths significantly outnumbered Israeli deaths. With suicide bombings, Palestinian groups raised the death toll for Israelis. Although suicide bombers carried out fewer than one percent of all anti-Israeli attacks, they were responsible for more than half of Israel’s casualties. Palestinian groups used suicide tactics with a considerable degree of popular support, and it was not long before Fatah and the Popular Front for the Liberation of Palestine (PFLP) joined in carrying out suicide bombings.

What stands out about this episode is the marked decrease in suicide attacks beginning in 2003. There has not been an end to terrorism in Israel nor an end to the ongoing Israeli-Palestinian conflict. The reduction in suicide bombings did not require the defeat of the groups that carried out so many of the attacks. The decrease likely resulted from a combination of efforts. The most effective were likely those that made it more difficult to carry out the types of attacks that had become commonplace during the Second Intifada, specifically the suicide bombings that had been inflicted upon otherwise peaceful cities in Israel.

**Preventing Suicide Attacks**

Israel’s COIN and counterterrorism operations during and after the Second Intifada preceded the abrupt end of most suicide attacks. Two efforts stand out. One was Israel’s reoccupation of parts of the Palestinian territories. Another was the creation of barriers, which impeded militants’ movements and coordination within and between the territories and limited their access to Israel. Reoccupation allowed Israel to regain access to human intelligence. Creating barriers allowed Israel to interfere with militants’ operations. While these were not the only tactics used by Israel, there are reasons to believe that these were the most effective in terms of reducing the incidence of suicide bombings.

As part of its COIN strategy, Israel’s military reentered areas that had been under Palestinian control. These included city centers within the areas known as “Category A” territories, which the Israel Defense Forces (IDF) had vacated years earlier as part of the Oslo Agreement. One of Israel’s objectives was to clear the densely populated refugee camps, neighborhoods, and city centers of Palestinian militants. The military’s progress through the Palestinian cities was organized and methodical. Israel’s ground forces surrounded the Palestinian communities and advanced house-by-house. They pressured militants toward a predetermined location from which they would be rounded up. Moving through the cities, Israel confiscated weapons and destroyed the facilities used to produce weapons, including bomb-making factories.

The progress continued day and night, with reinforcements for ground troops and, when feasible, support from large artillery on the ground and assistance from the air. Israel had at this time, and still has, one of the most capable militaries in the world. The Palestinian militants, by contrast, lacked coherence in training and leadership. They belonged to competing groups and gangs. Some were affiliated with the PA and PLO. Others were part of the opposition to the PLO. Some were criminal rather than political. In terms of resistance, the primary modus operandi for many of these groups was terrorism, with attacks carried out in secrecy, often with one or a few perpetrators directed by a local cell. As a result of the military incursion, the militants were forced to switch from their usual offensive posture to a defensive one. The Palestinian militants were poorly equipped for the fight that ensued. They lacked reinforcements, their supply lines were cut, and their weapons stocks were soon out of reach. The militants were essentially trapped with “nowhere to run.” Many were killed in the fighting. Once corralled, the Palestinians who were no longer fighting were subject to surrender
and arrest. Through this effort, the militant groups were weakened, though only in the short-term.

Even more importantly, in the interest of counterterrorism, reentry into these areas and reoccupation allowed Israel to reestablish direct access to human intelligence, which had been lost with the earlier withdrawal. Human intelligence gives context to information gathered through other types of monitoring, such as that collected through signal and visual intelligence, and tends to be superior in cases in which militant activities are plotted privately. Under Palestinian rule, would-be attackers, their handlers, and other militants could move with relative ease within and between the Palestinian-controlled areas. Militants could communicate in person and set-up operations outside the reach of Israel’s visual and signal intelligence.

After reoccupying the West Bank, Israel began building physical impediments to this coordination. This included the construction of barriers, including security fences, roadblocks, and checkpoints. Israel set out to separate militants from each other and from their potential targets. The barriers have done more than this. In addition to the disruptions they impose on terrorist activities, they also allow additional time for efforts to counter potential threats. Security fences separated Israeli and Palestinian communities, making it more difficult for Palestinians to enter Israel and Israeli-occupied areas. Israel established roadblocks and checkpoints along roadways connecting Palestinian communities within the West Bank, inhibiting Palestinians’ movement. Roads could be closed to traffic altogether, or they could be manned as checkpoints by Israeli soldiers. Checkpoints facilitated signal interceptions and added the additional constraint of direct surveillance. For would-be suicide attackers, this meant a higher probability of detection prior to carrying out an attack. For known militants, there was the added risk of being identified and detained. This combination was especially useful in cases in which attacks were known to be imminent.

In these ways, Israel limited access to the types of high-value targets Palestinian terrorists had previously sought. Would-be attackers could no longer expect to reach their preferred targets, the crowded civilian-filled destinations in Israel’s largest cities, unencumbered. Roadblocks and checkpoints interrupted the daily business associated with militant activities. They limited terrorists’ access to each other. Moving people and weapons became more difficult. Terrorists were no longer able to coordinate in person without fear of detection, or at least added surveillance. Other means of coordination, such as via phone or internet, remained subject to interception. With people on the ground within the Palestinian territories, signal and visual surveillance was again supplemented by human intelligence. Israel regained the capacity to identify threats before they materialized.

In the Gaza Strip, Israel removed settlements and established a security barrier. The result was little movement between the communities and an abrupt end to suicide bombings originating from Gaza. As Gaza was also Hamas’ and PIJ’s main base of operations, this also eliminated much of the threat of suicide attacks posed by these groups.

There was an added deterrence associated with the hardening of civilian targets. Israeli businesses, such as malls, clubs, and markets, maintained (and continue to maintain) trained security professionals, ready to intervene in cases of terrorist threats. This deterrence only slightly hardened these targets, perhaps stopping attackers at entrances rather than stopping attackers altogether. What made targets in Israel’s cities more difficult to attack was that they were much harder to reach.

Israel’s reoccupation of the Palestinian territories in the West Bank and construction of barriers did not end terrorism, nor did these efforts result in an immediate end to suicide attacks. They did, however, make suicide bombings much more difficult to carry out. As a result, suicide bombings became less common and less debilitating.
Alternative Explanations

Beyond effective COIN and counterterrorism operations, there are other possible explanations for the decrease in suicide bombings in Israel. For one, it is true that the decrease in suicide bombings corresponded with the end of the Second Intifada; however, the decrease has outlived the end of the Intifada. Violent resistance continues, but suicide attacks are an infrequent part of this violence. Second, the groups that first used suicide attacks did so during a time of relative peace and as a sign of opposition to Israel and the governing PLO. Given this, it would be conceivable that an end to the Intifada and a return to PLO-led governance would coincide with more attacks rather than fewer. Third, if suicide bombings were the best weapons available to the weaker militants, then it would make sense to see suicide bombings increasing instead of decreasing as the Palestinians were losing their fight. Adding to this, Palestinians were ending the Second Intifada in a weakened position, with less autonomy, less territory and, probably, less optimism than they had at the end of the First Intifada. A better explanation for the reduction in suicide bombings takes account of enhanced intelligence gathering, the lack of access to desirable targets, and the higher likelihood of mission failure following the reoccupation and construction or barriers.

Another possible explanation for decreasing numbers of suicide bombings draws on changes in public opinion regarding support for suicide attacks and political necessity. Suicide attacks were potentially costly in political terms for the groups carrying out the attacks, domestically as well as with international audiences. A decrease in suicide bombings could be explained by declining support for these tactics within the communities from which militants drew support. A return to political legitimacy after the Intifada could also help explain a shift away from suicide tactics.

A problem with this reasoning, however, is that changes in popular support cannot independently account for a decrease in suicide bombings. The groups that were most likely to be motivated by political considerations, including the affiliates of Fatah and the PFLP, joined in the use of suicide bombings at a time when the overall numbers of attacks were beginning to decrease. Moreover, if these groups were engaging in outbidding, essentially using increasing levels of violence to gain popular support, their participation should have corresponded with higher numbers of suicide bombings overall rather than fewer. In addition, repression, rather than preventing terrorism, may contribute to more terrorism as well as more support for terrorism. In fact, it was becoming more difficult to carry out suicide bombings, especially for the groups based primarily in the Gaza Strip and increasingly for groups operating in the West Bank, as well.

Another issue with this reasoning is that changes in popular support may not have a sizable influence on militants’ operations. Militants rely on popular support to some extent, or at least popular complacency, yet they also rely on support from other influential power holders. These may include clans in the Palestinian context. In other contexts, they may include tribes or other types of political entities. Also, to an important extent, terrorists have a tendency not to respect the opinions of the people whose interests they purport to represent. Again, representation is not understood in the democratic sense. Militant groups are authoritarian actors, guided by their own interests and ideas and often willing to use violence against their own people. Not only do the people residing under their control have few options in terms of representation, they also have few outlets for opposition.

Another possible explanation for the reduction in suicide attacks around 2005 is that changes in popular support toward the end of the Intifada may have resulted in fewer volunteers for suicide missions, or at least fewer capable volunteers. Volunteerism is one way to “voice” support for or opposition to militants’ activities. More likely, however, it would be an increasing likelihood of mission failure that would deter or reduce the supply of capable volunteers for these missions. If an individual-level logic for suicide attackers holds – if it is true that self-sacrifice will be celebrated, and that people participate in suicide attacks because
they wish to be celebrated as martyrs – then the potential benefits of these attacks would diminish with the decreasing likelihood of attack success. This is also consistent with the idea that the reduction in suicide bombings is associated with the deterrent effect of reduced access to targets.

Another pattern is worth noting. The reduction in terrorism, in general, during the Second Intifada appears to have coincided roughly with the reduction in suicide bombings. Suicide bombings made up a larger proportion of terrorist attacks between 2002 and 2004, and both suicide and non-suicide attacks declined in 2003 and 2004. However, while terrorism increased again in 2005, after the end of the Second Intifada, suicide bombings did not. Terrorists found new ways to attack Israel, such as with rockets fired from the Gaza Strip (coincidentally, an innovation that also belongs to Hezbollah). Rockets cross barriers that people cannot cross. Suicide bombers have not originated from Gaza and have been rare in the West Bank, especially since 2008.

Yet another possible explanation for the decrease in suicide bombings draws on another of Israel’s counterterrorism efforts during Operation Defensive Shield (ODS). Israel’s initial reoccupation, including the arrests, confiscation of weapons, and destruction of terrorist infrastructure, posed an immediate blow to Palestinian militancy. Adding to this, Israel’s long-held policy of targeted assassinations of terrorist leaders has weakened the most extreme groups. The problem with some of these explanations is that they do not independently explain the reduction in suicide bombings. The confiscation and destruction of weapons had a short-term impact. Militant groups have found ways to rebuild their weapons caches, yet the decline in suicide bombings has been a durable trend. In addition, Israel did not defeat or destroy the groups responsible for the spate of suicide attacks. The groups survived the campaigns of arrests and assassinations. Terrorist leaders were replaceable, and their foot soldiers, the suicide bombers who were less central to the organizations employing them were even more so. There is also evidence suggesting that terrorist attacks increased in the immediate aftermath of assassinations of terrorist leaders during the Second Intifada. In contrast, arrests of militants during the same time, which were facilitated by the newly erected barriers, including walls, roadblocks, and checkpoints, may have contributed to fewer suicide bombings. Human intelligence and effective barriers are among the reasons why suicide attackers were captured and their missions curtailed.

Taken together, alternative explanations, such as the end of the Second Intifada, changes in popular support, and losses of leaders and weapons, cannot independently account for the reduction in suicide bombings that began in 2003. It is more likely that with Israel’s reoccupation of the West Bank and construction of barriers, suicide bombings became much more difficult to carry out and no longer offered militants the potential payoffs they once enjoyed. The most valuable targets became increasingly difficult to reach. Fewer attackers would be capable of passing through checkpoints to complete a suicide attack.

Terrorism did not end with these efforts, nor did suicide attacks cease entirely. The same militant groups continue to operate, and the violence continues, yet suicide attacks are no longer a significant part of the story. Renewed access to human intelligence and the installation of barriers to militants’ movement and coordination more closely correspond to changes in the numbers of suicide bombings.

Conclusion

There are issues with applying lessons from these cases to other contexts or types of attacks. The case of Israel is unique in important ways, as is the case of preventing suicide hijacking missions. Both are narrowly-focused – one is focused on a unique context, the other on a specific tactic – and neither effort in prevention resulted in an end of terrorism, or even a reduction in terrorism. Neither effort resolved the reasons the groups responsible for suicide
attacks resorted to violence in the first place, nor did they prevent these same groups from continuing to use violence. Both efforts have been associated with high costs.

While the case of Israel provides an example of how one country effectively prevented most suicide bombings within its borders, the methods are not without problems. Israel’s approach, effective though it was at halting suicide bombings, required reasserting authority over Palestinian communities. Security fences, roadblocks, and checkpoints are among the inconveniences that impact Palestinians regardless of their participation in, or support for, militancy. One could argue that widespread support among Palestinians for militant groups equates with complicity; however, some of those militants were affiliated with the leadership of the PA government, which also enjoyed support and legitimacy outside the Palestinian territories as a negotiating partner and leader of the post-Oslo government.

Assigning guilt to Palestinians as a group is also an oversimplification on par with blaming any people for the acts of their government. Such culpability, of course, assumes that the people have influence over their government. Palestinians, as a group, have limited influence. They do not reside in a democracy. The people did not elect their initial PLO-led government. They have had few opportunities to influence governance and few options in terms of representation, even in the post-Oslo era. As the Palestinian national elections of 2006 showed, the only viable alternative to the PLO and Fatah’s control of the Palestinian Authority was Hamas, and Hamas’ electoral successes in that election, in which it won a majority in the PA’s parliament, cost Palestinians much of the foreign support on which they had relied. One could argue that Palestinians are simultaneously victims of the ongoing conflict with Israel as well as of their own militant groups and the parties purporting to represent their interests.

There is another significant limitation of the discussion of Israel’s operations. There are unlikely to be many opportunities to apply lessons learned in Israel to other cases. Few contexts resemble Israel and the Palestinian territories. Collecting intelligence, constructing barriers, and policing an entire population require considerable capacity, which Israel has. The Palestinians are both concentrated within territories, and divided between them. Their political leadership is also divided and relatively weak. Israel has a limited geographic space to oversee. Despite this, while Israel’s COIN and counterterrorism operations provide the state with some level of security, this security is gained at Palestinians’ expense and comes with the added cost of continued violence.

Preventing suicide attackers from using commercial airplanes has also come at a cost, though these costs and their benefits are borne, and enjoyed, largely by air travelers. Among the costs are those associated with redesigning airports, implementing security screening protocols along with new technologies, and employing the variety of screeners and other security personnel required to make these efforts effective. Closing the security gaps exploited by the 9/11 attackers required rethinking the nature of threats while building on existing security measures. It is possible to apply lessons from preventing attacks on air travel to the prevention of attacks on other types of targets. Some of the measures used for hardening air travel have been employed with other forms of mass transit, such as with train travel, creating further barriers to attacks on these targets.

Despite successes, there are other issues associated with preventing suicide attacks by terrorists, which neither the case of Israel nor the case of increasing security at airports addresses. One such issue is ongoing support for suicide attacks and the groups using them. Efforts to prevent suicide attacks have not removed support for the types of violent resistance associated with these attacks, or with terrorism, in general. Israel halted suicide bombings, for the most part, but did not remove threats of terrorism. The hardening of air travel stifled attacks and attempted attacks on airplanes and airports, but the group associated with the perpetrators of the 9/11 attacks has not been defeated. While its central command has been significantly weakened, al Qaeda’s presumed ‘network’ has expanded since 9/11, and numbers of terrorist attacks, including suicide terrorist attacks, have increased with the expansion of these groups’
operations. Efforts to eliminate these groups and their competitors, including factions and former affiliates, have coincided with an increase in suicide attacks and an increase in terrorism.

Neither the hardening of potential targets, which is an inherently defensive measure, nor the implementation of targeted military operations, which is an inherently offensive approach, is geared toward removing the grievances that fuel ongoing violent resistance. In fact, in important ways, both efforts have the capacity to augment grievances, such as can be observed among Palestinians, and increase insecurity and state weakness, as can also be observed in Iraq and Afghanistan.

This discussion may seem to suggest that lessons taken from past efforts at preventing suicide attacks by terrorists have limited applicability to future efforts. The value, however, comes from consideration of what has worked in the past and what may work better in the future. Much of the effort discussed here has been reactive. While counterterrorism responses have sought to remove vulnerabilities, terrorists have found new vulnerabilities to exploit, requiring further reaction. The terrorists that have used suicide attacks will adapt and innovate. The violence will continue, though it may take new forms. To be effective, efforts to counter terrorism will also require innovation and adaptation.

Dr. Susanne Martin is an Associate Professor of Political Science and Director of the International Affairs Program at the University of Nevada, Reno. In addition to her work on prevention, Susanne Martin’s work on suicide attacks also includes studies of the history of suicide tactics in warfare and analyses of changes in suicide tactics. Susanne Martin also works on themes relating to political violence and warfare, more generally, with a focus on the groups that engage in violent activities, the conditions under which groups use violent versus nonviolent tactics, and the types of groups that are more likely to abandon violence. Insurgent groups and terrorist groups are the focus of much of her work, along with the political parties with which some of these groups have affiliations. Professor Martin is co-author (with Leonard Weinberg) of The Role of Terrorism in Twenty-first-century Warfare (Manchester University Press, 2016). In this work the authors explore patterns in the timing of terrorism within wider-scale warfare. Susanne Martin is also author of “Dilemmas of ‘Going Legit’: Why Should Violent Groups Engage in or Avoid Electoral Politics?” (2014), published in the journal Behavioral Sciences of Terrorism and Political Aggression. She is also a student of language, with formal training in German, Spanish, Serbian, Bosnian, Croatian, French, and Czech. Professor Martin earned her doctorate in Government at the University of Texas at Austin.
Endnotes


9 Boot, 2013, pp. 569-570.

10 See, for instance, De la Calle, Luis, and Ignacio Sanchez-Cuenca. ‘What we talk about when we talk about terrorism’, Politics and Society 39.3 2011, p. 458.


13 Ibid.

14 Ibid.

15 Ibid., p 20. We can expect there to be cases in which suicide attacks have involved unwilling participants, though we may not be able to distinguish these from those attacks with willing participants. There is often too little information to rule out remote detonation and forced participation, and ‘successful’ suicide bombers cannot provide this information.

16 Similarly, there are many occasions on which states have used suicide attacks in regular warfare, especially toward the end of a war and when defeat was almost inevitable. This was the case toward the end of the Second World War, when Japanese kamikaze pilots attacked American warships in the Pacific.
Suicide missions such as those described by Japan’s kamikaze pilots were not terrorism but rather part of the warfare between states. In addition, the kamikaze pilots used planes as explosives, more along the lines of the 9/11 attackers. The suicide bombers in Lebanon carried their explosives or used cars.


See, for instance, Moghadam, 2006.

The Tamil Tigers had eliminated Tamil opposition and consolidated power within their organization. With their defeat, the organized Tamil opposition in Sri Lanka also dwindled.


For example, Rapoport 2012.

For example, Weinberg 2005, Chapter 2.

Weinberg 2005, Chapter 3; Rapoport, 2012, p. 52.

Kurzman, Charles, ‘Why is it so hard to find a suicide bomber these days?’ *Foreign Policy,* 2011, p. 188.


Frisch 2006, p. 867


Ibid., p. 373.

See, for instance, Byman and Pollack, 2007, p. 25.


See, for example, Pedahzur 2005, p. 52.

See, for example, Pape 2005, pp. 130-133, pp. 253-254 (Appendix 1).

See, for example, Ricolfi 2005, p. 88.


See, for example, Ricolfi, 2005, p. 89; Bloom, Mia, ‘Palestinian Suicide Bombing: Public Support, Market Share, and Outbidding’. *Political Science Quarterly,* 2004, 119:1, p. 68.

Available at: https://www.rand.org/pubs/monographs/MG146-1.html (last accessed July 2020).

61 Ibid., pp. 51-53.
63 Ibid., p. 53.
64 Levin 2018, pp. 57-58.
68 Global Terrorism Database 2020; Pape 2005, pp. 253-257, 260-262 (Appendix 1).
70 Global Terrorism Database 2020.
71 Ibid.
72 Ganor, p. 5.
73 See, for example, Bloom, 2004, p. 73.
74 See, for example, Byman, Daniel, ‘Curious Victory: Explaining Israel’s Suppression of the Second Intifada.’ *Terrorism and Political Violence* 24:5, 2012, p. 826. In contrast to arguments that occupation is a cause of suicide terrorism, Byman describes Israel’s effort to prevent suicide bombings as effective because the state was “increasing the extent of its occupation.”
75 See, for instance, Perliger, Arie, and Ami Pedahzur, ‘Coping with Suicide Attacks: Lessons from Israel.’ *Public Money and Management* 2006, 26:5, pp. 282-283.
80 See, for example, Jones 2007, pp. 290-291.
81 See, for example, Jones 2007.
82 Catignani 2005, p. 256.
84 Jones 2007, p. 294.
85 See, for example, Byman 2012.
86 Ibid., pp. 832-833.
90 See, for example, Perliger et al. 2009; Jones 2007, pp. 250-251.
See, for example, Jones 2007, pp. 291-294.

See, for example, Perliger et al. 2009, pp. 1293-1294.

Pape 2005, pp. 9-11.


See, for instance, Bloom 2004, pp. 72-76.


See, for example, Bueno de Mesquita, Ethan. ‘The Quality of Terror’, *American Journal of Political Science*, 2005, 49:3. Bueno de Mesquita argues that terrorist groups seek to employ the best, or most capable, among those who volunteer. He further asserts that increasing rewards may coincide with more capable volunteers within the pool of potential recruits, as observed during the Second Intifada (pp. 524-525).


Global Terrorism Database 2020.


Bibliography


Ganor, Boaz. n.d. ‘The Rationality of the Islamic Radical Suicide Attack Phenomenon’. In: Countering Suicide Terrorism (Herzliya, Israel: IDC Herzliya, Institute for Counterterrorism, ICT), pp. 5-11.
Global Terrorism Database (GTD) (2020). National Consortium for the Study of Terrorism and Responses to Terrorism (START). Available at: https://www.start.umd.edu/gtd/access/ (last accessed July 2020).


Horowitz, Michael C., ‘Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism’. International Organization 64.1, 2010 pp. 33-64.


Kurzman, Charles, ‘Why is it so hard to find a suicide bomber these days?’ Foreign Policy 188, 2011, pp. 1-10.


Web-based Resources

Chicago Project on Security and Terrorism (CPOST), University of Chicago. Available at: cpost.uchicago.edu/
Combating Terrorism Center at West Point, United States Military Academy at West Point. Available at: etc.usma.edu/
“Country Reports on Terrorism,” United States Department of State. Available at: www.state.gov/country-reports-on-terrorism-2/
Global Terrorism Database (GTD), National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland. Available at: www.start.umd.edu/gtd/access/
“Global Terrorism Overview: Terrorism in 2019,” Background Report, National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland. Available at: www.start.umd.edu/pubs/START_GTD_GlobalTerrorismOverview2019_July2020.pdf
International Centre for the Study of Radicalisation (ICSR), Department of War Studies, King’s College London. Available at: icsr.info/
“Mapping Militant Organizations,” Center for International Security and Cooperation (CISAC), Stanford University. Available at: cisac.fsi.stanford.edu/mappingmilitants/mappingmilitants
National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland. Available at: www.start.umd.edu/
RAND Corporation, “Suicide Attack.” Available at: www.rand.org/topics/suicide-attack.html
RAND Corporation, “Terrorism Threat Assessment.” Available at: www.rand.org/topics/terrorism-threat-assessment.html
Chapter 26

The Terrorist Threat to Transportation Targets and Preventive Measures

Brian Michael Jenkins

Attacks on airliners and airports constituted a large percentage of terrorist operations in the late 1960s and early 1970s, requiring extraordinary security measures. Despite progress in reducing the number of hijackings and sabotage of airliners, terrorists continued to attack commercial aviation. The 9/11 attacks in which nearly 3,000 people died, and subsequent suicide bombing attempts aboard airliners prompted even more stringent measures to keep weapons and explosives off airplanes. By 2020, terrorist hijackings have been almost entirely eliminated although sabotage remains a concern. Meanwhile, terrorist attacks on public surface transportation steadily increased into the 2010s. The attacks in the early 1970s were aimed at causing alarm and disruption. To later generations of terrorists, trains and buses offered easily accessible crowds of people in confined environments—the goal changed to slaughter as witnessed in the bombings of commuter trains in Madrid in 2004, London in 2005, and Mumbai in 2006. The aviation security model could not be applied to surface transportation. The volume of passengers was too great—passenger screening would require an army of screeners. The delays and costs would destroy public transportation. Instead of establishing security checkpoints, transportation operators had to look at ways to mitigate casualties through station and coach design and rapid intervention, and enlist passengers themselves in detecting suspicious behavior and objects.

Keywords: aviation, buses, hijackings, passengers, prevention, railways, security, terrorism, transit, transportation
Terrorism can be examined from various perspectives. Analysts have studied the causes that motivate terrorist campaigns, the radicalization process by which individuals move from extreme beliefs into the realm of actually using violence, the *modus operandi* of various terrorist groups, the evolution of terrorist tactics, the unique challenges terrorists pose to security, and the legal responses and other countermeasures. In this chapter, we examine terrorist targeting of commercial aviation and surface transportation. The terrorists’ focus on this set of targets tells us a great deal about their strategies.

Attacks on airliners and airports constituted a large percentage of terrorist operations in the late 1960s and early 1970s, and these targets appear to be a continuing obsession for some terrorist groups, necessitating extraordinary security measures. Terrorist attacks on passenger trains, metros, and buses also began in the early 1970s, and they increased in volume and lethality during subsequent decades.

In going after transportation targets, terrorists are not making statements against any particular mode of public transportation. Targeting airplanes or passenger trains reflects broader objectives and trends. Commercial aviation has offered accessible targets to terrorists who had little chance of operating inside the countries whose governments or policies they opposed. Like embassies and diplomats - also favorite targets of terrorists in the 1960s and 1970s - airplanes are symbols of the enemy, vulnerable outposts that can be attacked anywhere in the world. In addition, attacks on international air travel guarantee worldwide publicity.

The increase in attacks on surface transportation, which came later, reflected different trends. As terrorists sought to escalate their body counts and were willing to kill indiscriminately to do so, trains and buses became convenient killing fields. Symbolism was less important than accessible crowds of people aboard trains or subways or in stations or depots. Instead of attacking symbolic targets abroad, attacks on surface transportation targets were carried out by local operatives - homegrown terrorists - although some were inspired by the actions of known terrorist groups and some were assisted from abroad.

**Terrorists Make Commercial Aviation Part of the Battlefield**

Commercial aviation offered terrorists mobility and targets in the 1960s. Jet air travel, which had expanded rapidly in the preceding decade, offered terrorists the opportunity to board an airplane in one country and then fly to another country, where they could hijack a second airliner and divert it to a third country.

Commercial airliners also provided terrorists with nationally labeled containers of hostages, increasing their leverage over target governments. When sabotaging airliners, terrorists could punish a country by achieving high body counts. Airlines and airports found themselves on the front line of a global conflict. This is still the case.

Terrorism in its contemporary form emerged with a series of spectacular attacks in the late 1960s. Airline hijacking entered the terrorist repertoire in July 1968, when members of the Popular Front for the Liberation of Palestine (PFLP) hijacked an El Al airliner and forced it to fly to Algiers, where they released the non-Israeli passengers but demanded the release of convicted Arab prisoners held by Israel in return for the safe release of the remaining passengers and crew.¹

The episode, which lasted 40 days, was not, however, the first hijacking of a commercial airliner. After World War II, hijacking had often been employed as a means to escape from the Soviet Union and other countries behind the Iron Curtain, and during the 1960s, flights in the US were frequently hijacked by individuals wanting to fly to Cuba. But the El Al incident was the first hijacking to involve political demands beyond asylum, and it set off a wave of terrorist hijackings.

The PFLP struck again in August 1969, hijacking a plane on a flight between Rome and Tel Aviv and flying it to Damascus. In September 1970, the PFLP escalated its campaign,
hijacking three commercial airliners and flying them to an airfield in Jordan that was under Palestinian control. As part of the same operation, PFLP operatives hijacked a fourth plane and flew it to Egypt. A fifth hijacking was foiled when PFLP hijackers were shot by Israeli air marshals while trying to take control of an El Al plane. Airline hijacking became increasingly common between 1968 and 1972, when hijacking attempts occurred with an average frequency of one every six days.

Airline sabotage entered the terrorists’ playbook in February 1970, when the PFLP planted a bomb aboard a Swissair jet flying from Zürich to Tel Aviv. The arrest and conviction of three Palestinians by Switzerland had made the country a target for retaliation. The explosion caused the plane to crash, killing all 47 persons on board. The same day, another bomb smuggled by the PFLP into the cargo hold of an Austrian Airlines flight from Frankfurt to Vienna exploded, blowing a hole in the side of the aircraft, but the captain managed to keep the plane under control and bring it to a safe landing.

Airports also became part of the battlefield. In May 1972, three members of the Japanese Red Army recruited by a Palestinian group arrived at Tel Aviv’s airport on a flight from Rome. Taking automatic weapons and hand grenades out of their hand luggage, they opened fire on passengers and airport staff, killing 26 people and wounding 80, many of them Puerto Ricans on their way to the Holy Land. It was not merely the scale of the carnage from the event that attracted global attention, but its international complexity. How was it, people asked, that Japanese terrorists came to Israel to kill Puerto Ricans on behalf of Palestinians?

The attacks on commercial aviation fit into the broader strategy of the Palestinian groups determined to carry on an armed struggle with Israel. Tight security made it difficult for Palestinians to carry out attacks inside Israel itself, but there were ample Israeli and Jewish targets abroad. Attacking airlines flying to Israel or belonging to countries perceived to be supporting Israel’s existence was, in the eyes of the Palestinian attackers, a legitimate expansion of the battlefield and had historical precedence.

The early Palestinian groups modeled their own struggle on the Algerian war for independence (1954-1962). The Algerians had carried their armed struggle beyond the colony of Algeria to the metropole - France itself. The Palestinians saw Israel as a colony imposed on them by the West. If Israel itself was too hard a target, the Palestinians would attack Israel’s support structure abroad - Zionists, which in Arab eyes included Jews anywhere, nations supporting Israel (which meant nations not supporting the Palestinians), countries doing business with Israel, and travelers to Israel. All were considered “legitimate” targets. There were no innocents.

Although the Palestinian groups were innovators and the most frequent attackers, they were not alone in targeting aviation. Other groups followed their lead. The Japanese Red Army, independently of its alliance with the PFLP, hijacked airliners. Marxist guerrillas in Latin America and Europe, along with Eritrean, Croatian, Armenian, Puerto Rican, and Kashmiri separatists, Sikh extremists, and anti-Castro extremists also attacked airliners and airports in the 1970s. In addition, there were individual hijackers seeking asylum, demanding ransoms, escaping law enforcement, or calling attention to personal grievances. In some cases, their motives remain unclear. The hijacking phenomenon was widespread.

**Extraordinary Security and International Cooperation**

The continuing threat required extraordinary security measures. Israel decided that it could not risk the hijacking of another El Al airplane and made airline security a matter of national security. El Al implemented screening procedures that included interrogating boarding passengers. The airline’s comparatively small number of international flights and the composition of its passenger load made this approach feasible. Armed air marshals provided an additional layer of security.
Other commercial airlines were reluctant to adopt such stringent measures, but by 1973, as hijackings continued, government regulatory authorities compelled the airline industry to adopt 100-percent passenger screening. More frequent flights, a greater volume of passengers, a more diverse flying population, public resistance, and privacy concerns obliged the industry to adopt less-intrusive inspection techniques than those implemented by the Israelis, however. Instead of attempting to profile passengers according to risk, airline security treated everyone equally and instead looked for weapons and explosives.

By today’s standards, early aviation security was primitive. It consisted of metal detectors to keep weapons from being smuggled aboard flights and x-ray or physical inspection of carry-on luggage. Explosives detection technology was not routinely deployed until the 1990s. Body scanners were deployed after 2010, and imaging technologies have been steadily improved.

Parallel with the increased security measures adopted by different countries, the proliferation of attacks on commercial airliners in the late 1960s and early 1970s also led to efforts to increase cooperation at the international level. A single event could involve the governments of several countries, so prevention and resolution of incidents required international coordination.

The Convention on Offences and Certain Other Acts Committed on Board Aircraft, commonly called the Tokyo Convention, was introduced in 1963, when hijackings were still only occasional events. It was the first international agreement that addressed security and gave the captain of a flight authority to deal with passengers who jeopardized the safety of the flight. It also required countries where hijacked or threatened aircraft landed to restore the authority of the captain and take the offender into custody until extradition could be arranged. Ratification was slow. By 1969, only about half of the world’s countries had ratified the Tokyo Convention.

The increase in hijackings and sabotage attempts in 1969 and 1970 called for new measures. During the two-year period, there were 118 hijackings and 14 incidents of sabotage. The 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft obligated states to either prosecute or extradite hijackers, thereby closing off safe havens such as Cuba. The Hague Convention was widely adopted but did not cover aircraft sabotage.

This gap was filled by the 1971 Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, which extended criminal culpability to individuals not on board the aircraft. A separate protocol in 1988 extended the convention to crimes at international airports.

These conventions were part of a broader international effort to outlaw all international terrorist tactics. In addition to the conventions and protocols covering commercial aviation, conventions outlawed attacks on diplomats, taking hostages (already a war crime under the 1949 Geneva Convention), attacks on maritime targets and offshore platforms, and terrorist bombings (which were defined as bombing places of public use, government facilities, public transportation systems, or infrastructure facilities). By the end of the century, there were also international agreements to protect nuclear material, mark plastic explosives to aid in investigations, and prevent terrorist financing.

Ratification by individual states and compliance with the agreements varied greatly, but overall, the corpus of anti-terrorist conventions signaled that the international community did not want to see progress that had been made in regulating armed conflict reversed by terrorism, and the conventions facilitated cooperation where there was political will to cooperate. International cooperation on dealing with attacks on commercial aviation did improve, due to a combination of international agreements and diplomatic pressure on uncooperative states.

The combination of increased security (though costly and inconvenient), international cooperation (although uneven), and the suppression of some of the groups responsible for hijackings appeared to gradually reduce the number of hijackings. As pointed out in 1998 in *Aviation Terrorism and Security*, airplane hijacking dropped from an average of 50 events a
year in the late 1960s to an average of 18 in the 1970s and 1980s and an average of 14 in the 1990s. Although the numbers differ slightly, a more recent (and excellent) analysis by Jacques Deuchesneau shows a jagged decline from a high point in 1970. Looking at it another way, attacks on commercial aviation, which accounted for roughly a third of terrorist attacks on all targets in the late 1960s, declined to just 7 percent of terrorist attacks in the 1970s.

However, Ariel Merari, a distinguished Israeli authority on terrorism, noted that “despite the long-accumulated experience with attacks on commercial aviation and notwithstanding the immense investment in security measures and procedures, the effectiveness of aviation security measures has not improved during the past three decades [1967–1996].” Merari did not challenge the fact that the number of airline hijackings had declined from its peak at the beginning of the 1970s, but he pointed out that the number of successful attacks remained unacceptably high.

Moreover, the rate of thwarting hijackings had not improved. In the decade between 1967 and 1976, 31 percent of all attempted hijackings were thwarted. In the decade between 1987 and 1996, only 18 percent were thwarted - the most determined hijackers were still getting through security. Terrorist bombers were also getting through.

**Aircraft Sabotage**

While terrorist hijackings declined, attempts to sabotage aircraft increased. In 1974, a bomb caused the crash of a TWA flight from Tel Aviv to New York, killing all 88 on board - the bloodiest terrorist attack to that date. In 1982, an offshoot of the PFLP planted bombs aboard two Pan Am flights. One bomb exploded on a flight between Tokyo and Honolulu. The explosion killed one passenger and wounded 14 others, but the pilot was able to land the plane safely. Two weeks later, cleaners discovered an undetonated device on a Pan Am plane at the airport in Rio de Janeiro. These bombs and others detonated later in the decade were the work of a single terrorist bombmaker who, despite a multi-million-dollar reward, was never arrested.

The deadliest act of terrorism involving aviation prior to the 9/11 attacks on New York and Washington, DC, occurred in June 1985, when Sikh extremists bombed an Air India flight from Montreal to London, killing all 329 people on board. On the same day, that group also had attempted to sabotage another Air India flight scheduled to take off from Tokyo, but the device they planted exploded prematurely, killing two baggage handlers.

Further incidents of aircraft sabotage occurred in the 1980s and 1990s, including the 1987 bombing of a Korean Air flight, in which 115 people died; the 1988 bombing of Pan Am 103 over Lockerbie, which killed 270 people; and the 1989 bombing of a UTA flight to Paris, which killed 170. North Korean agents were responsible for the 1987 bombing, while Libyan agents were held responsible for the Pan Am and UTA bombings. These attacks paralleled the general escalation of terrorism in the 1980s.

Bringing down wide-body jets can potentially give terrorists a body count of several hundred. Exceeding this ceiling required multiple coordinated attacks. The most ambitious of these was the so-called Bojinka plot uncovered by Philippine authorities in 1995. The plot involved operatives planting bombs on 12 airliners flying to the US from various airports in Asia. The bombs were intended to produce near-simultaneous explosions over the Pacific. Had the plot succeeded, it could have resulted in 4,000 fatalities.

The Bojinka plot bombers perfected a small bomb suitable for the task, tested it on an Air Philippines flight, and were preparing to complete construction of the devices when an accidental chemical fire brought fire crews to their apartment laboratory in Manila. What the crews found aroused their suspicions and police were called in. One of the plotters was immediately arrested, and others were arrested after a manhunt. However, one of those involved in the plot escaped and later became the architect of the 9/11 attacks.
The Lead up to the 9/11 Attacks

The deadliest terrorist operation involving commercial aviation was the assault of 9/11. The audacious operation was the culmination of trends and ambitions expressed in terrorist plots and playbooks during the previous decades - airline hijackings, suicide attackers, multiple targets struck simultaneously to demonstrate organizational capacity and achieve a higher body count, an order-of-magnitude increase in the number of fatalities.

Authorities in the US said that the 9/11 scenario was a new type of attack that had not been foreseen. Although this precise attack was not predicted, the possibility of hijacked airliners crashing into buildings was neither unimaginable, nor unimagined. There were ample precedents, although they went largely unnoticed.

In 1972, three hijackers took over a Southern Airways flight shortly after takeoff from Birmingham, Alabama, initiating the longest hijacking saga in US history. On one of the flights, the hijackers threatened to crash the plane into the nuclear facilities in Oak Ridge, Tennessee. Atomic reactors were shut down immediately upon receipt of the threat. This case led to the imposition of passenger screening in the US.

In 1973, Israeli jets shot down a Libyan Arab Airlines plane that flew over Israeli-occupied territory in the Sinai, fearing that it might be deliberately crashed into Tel Aviv. In 1979, a Serbian nationalist hijacked a flight in the US. He demanded and received another airplane, which he ordered to fly to Ireland. From there he wanted the plane flown to Yugoslavia, where he planned to crash it into headquarters of the Communist Party in Belgrade.

In 1986, members of the Abu Nidal Organization, a Palestinian group based in, and supported by, Libya, stormed aboard a Pan Am jumbo jet preparing to take off from the Karachi airport in, Pakistan. The hijackers had intended to fly the plane to Israel and crash it into Tel Aviv. However, the pilots were able to escape from the cockpit. Without pilots, the hijackers could not fly the aircraft, and Pakistani commandos stormed the plane.

In 1993, an FBI informant and an ex-Egyptian Army officer, testifying at the trial of the plotters of a series of terrorist attacks in New York that were to follow the bombing of the World Trade Center, described another terrorist plot. According to the informant, a Sudanese Air Force pilot was to hijack an airplane, bomb Egypt’s presidential palace, and then crash the plane into the US embassy in Cairo. The plot never got beyond the discussion stage.

In April 1994, an off-duty pilot riding as a passenger on a Federal Express flight attacked the flight crew and attempted to crash the plane into a company building in Nashville, Tennessee. Later that year, a suicidal pilot with a history of alcohol and drug abuse crashed his single-engine Cessna onto the South Lawn of the White House, slamming into the White House itself. Then, in December, Islamist extremists hijacked an Air France jet departing from Algiers. According to French authorities, the hijackers had discussed crashing the plane into the Eiffel Tower, although exactly how this was to be accomplished is not clear. French commandos stormed the aircraft after it landed for refueling in Marseilles.

The most dramatic part of the 1995 Bojinka plot was the bombing of 12 airliners flying across the Pacific, but another part of the plot contemplated crashing a light aircraft into CIA headquarters. This idea was later proposed to Al-Qaeda leader Osama bin Laden, but he rejected it as paltry.

American intelligence services obtained information about a planned suicide attack by followers of the imprisoned instigator of the 1993 World Trade Center bombing and other terrorist plots in the US. The plotters intended to fly to the US from Afghanistan and attack the White House. Similar reports came to the attention of the intelligence community during the 1990s, including a reported plot in 1998 by Arab extremists to fly an explosives-laden plane into the World Trade Center. Authorities dismissed the plot as unlikely, and the existence of intelligence reports does not mean that all of the plots were serious. Nonetheless, the reports indicate that at least some terrorists were talking about scenarios involving crashing hijacked airliners into buildings of iconic value.
The architect of the 9/11 attack initially planned to crash 10 hijacked airliners into both the east and west coasts of the US, but this idea was abandoned as too complicated. Instead, the planners substituted the idea of a second wave of attacks involving hijackings or sabotage of aircraft. The intense reaction of the US to the 9/11 attacks rendered this impractical. However, Al-Qaeda did attempt a further round of sabotage attacks later in 2001. British volunteer Richard Reid was equipped with a small bomb concealed in his shoe, which he tried to detonate aboard a US-bound flight from Paris in December 2001. The device failed to detonate. A second bomber who was to detonate his device on a flight to the US from Amsterdam, changed his mind and abandoned his device.

### Dramatic Changes in Airline Security after 9/11

Not surprisingly, the 9/11 attacks prompted dramatic increases in aviation security. In the US, passenger screening, which had been conducted by contract services widely seen as inadequate, was taken over by the federal government. Inspections were heightened everywhere. Cockpit doors were armored and kept locked while the plane was in flight. The airline strategy for dealing with hijackings changed from compliance with hijackers’ demands to resistance if possible. Passengers became part of the response. Airline crews were empowered to enlist able-bodied assistants in dealing with threatening situations. Terrified passengers were ready to tackle and subdue hijackers themselves without waiting for an invitation or instructions by the crew. Hijackings declined.

There were 47 attempted hijackings of commercial airliners between 9/11 and March 2020. This continued the downward trajectory of hijacking attempts. About two-thirds of the attempts occurred in developing countries, some in conflict zones or theaters of ongoing terrorist campaigns. However, the hijackers were members of known terrorist groups in only a few cases. Most of them had personal motives; 25 had mental-health issues.

In 15 cases, the hijackers used knives or other sharp objects, including small wooden stakes, sharpened aluminum canes, a nail file, and a fountain pen, to threaten the crew. In only four cases were hijackers able to smuggle firearms past security, but three of them were in Sudan and Mauritania - both open conflict zones. In two more cases, the hijackers had replica guns or a toy pistol. Nine hijackers falsely claimed to have explosives. Crew and passengers overpowered the hijackers in several incidents. Apart from the hijackers themselves, no one was killed in any of these incidents. These figures underscore the continuing threat, but they also indicate that terrorist groups - who historically have accounted for only a fraction of the total hijackings - are playing an even smaller role. Security measures, where rigorously followed, appear to be having a measure of success in keeping guns off airplanes, but not in all cases. Cabin crew and passengers are now definitely part of aviation security.

After 9/11, governments also accelerated the deployment of explosives-detection technology, and after the attempted sabotage by the shoe bomber, passengers were required to remove their shoes during screening. Still, continuing sabotage attempts underscored the continuing threat.

In 2004, female suicide bombers simultaneously brought down two jets on domestic flights in Russia, killing all 90 persons on board. The discovery in 2006 of a plot in England to bomb airliners by using liquid explosives led to restrictions on the amount of liquids passengers could carry on board. An attempt in 2009 to blow up a US-bound airliner by a saboteur using a bomb concealed in his underwear led to the deployment of full-body scanners. In 2010, intelligence efforts in the Arab peninsula foiled terrorist plots to use bombs concealed in printer ink cartridges to sabotage airliners. Another attempt was foiled in 2012. Later intelligence reports indicated that terrorists were trying to conceal tiny but powerful bombs in laptops.
The fact that terrorist bomb makers were trying to develop tiny devices that would escape detection confirmed that despite criticism that airline security was ineffective and merely for show, terrorists took it seriously. And while terrorists were often able to smuggle their devices on board, the devices were generally unreliable.

Yet in 2015, a bomb smuggled on board a chartered Russian tourist airliner on a flight from Egypt to Russia detonated, killing 224 people. A bomb planted in the cabin of a passenger plane flying from Mogadishu, Somalia, in 2016 exploded, blowing a hole in the side of the aircraft and killing one passenger, but the pilot was able to land the plane. A month later, a soldier searching airline luggage was killed by another bomb.

Airports also remained targets. Terrorists and mentally unstable individuals carried out bombing and shooting attacks in the publicly accessible areas of airports in Los Angeles in 2002, Moscow in 2011, Brussels and Istanbul in 2016, and Fort Lauderdale, Florida, in 2017. These attacks led to a discussion of whether the security screening checkpoints should be extended to the front doors of terminals and whether outer perimeters should be added.

The idea of moving the screening checkpoints was rejected. Their purpose is to keep weapons and explosives off airplanes, not out of airports. Installing additional checkpoints to protect the publicly accessible areas of a terminal would have to cover both entrances and check-in areas, as well as baggage retrieval areas, and would risk creating crowds of people waiting to get through security who would be vulnerable to shootings or bombings.

Looking at the issue of airport security more broadly, any security measure against terrorism should provide a “net security benefit,” that is, it should not merely displace the risk from one crowded public place to another. If denied access to one venue, terrorists can target another to achieve the same results; in that case, there is not a net security benefit. An argument can be made that keeping adversaries from hijacking or bombing airplanes provides a net security benefit, while protecting the public areas of airports merely displaces the risk. The net-security-benefit argument is significant in the case of security of train stations and bus depots, discussed below.

Nonetheless, many airports have increased security at entryways, deploying more surveillance and armed guards to intervene rapidly in the event of a shooting. Rapid intervention to mitigate casualties differs strategically from prevention, which is what screening of boarding passengers and baggage aims at.

**The Threat Posed by Hand-held Surface-to-Air Missiles**

In the late 1970s, terrorism analysts tried to identify military weapons that terrorists might acquire and use in future attacks. One obvious concern were man-portable, precision-guided surface-to-air missiles, which were then being deployed in large numbers to armies around the world. As second- and third-generation weapons were distributed to the military establishments of the major powers, first- and second-generation weapons were sold to armies in developing countries, in many of which there were concerns about corruption and black-market sales. Terrorists had already acquired shoulder-fired anti-tank weapons.  

Despite these concerns, the US distributed Stinger missiles to the Afghan resistance fighters in 1986, which enabled them to shoot down Soviet helicopters. This altered the course of the war and the Soviet Union withdrew from Afghanistan three years later. As terrorism concerns grew after that conflict ended, efforts were made to account for and recover any remaining missiles. Concerns about terrorism precluded the distribution of surface-to-air missiles to the rebel formations during the civil war in Syria.

Guerrilla forces and terrorist groups did acquire some missiles and used them against commercial aircraft, but almost all of those incidents took place in conflict zones such as Rhodesia/Zimbabwe, Mozambique, Lebanon, Afghanistan, Sri Lanka, and Iraq. There were several reports in the 1970s and 1980s that terrorist groups had acquired surface-to-air missiles,
and for brief periods, airliners flying into certain airports adopted approach and takeoff procedures aimed at reducing their vulnerability footprint.

When TWA Flight 800 exploded in midair off the East Coast of the US in 1995, some speculated that it had been brought down by a missile. Anomalies in some of the physical wreckage lent weight to the assertion. Ultimately, however, investigators concluded that the plane had been brought down by an accidental explosion in the plane’s center fuel tank; nevertheless, the missile theory persisted. In its 1996 report, the White House Commission on Aviation Safety and Security recommended that a task force be created to assess the surface-to-air-missile threat, but the feared scenario of terrorists shooting down commercial airliners as often as they bombed planes did not come to pass.20 In 2002, Al-Qaeda operatives in Mombasa, Kenya, bombed a hotel and simultaneously launched two Soviet Strela missiles at a chartered passenger plane carrying Israeli tourists, but the missiles missed their targets. The attack, however, renewed discussions of countermeasures, including fitting commercial airliners with the anti-missile technology used by combat aircrafts.

### The Future of Aviation Security

Aviation security remains one of the most important components of our overall defense against terrorism. It is costly, controversial, and contentious. It dramatically demonstrates the basic tenet of terrorism - that small groups with a limited capacity for power can achieve disproportionate effects by using terrorist tactics. The threat of one terrorist bomber obliges the nation to divert vast sums to airport security. Terrorists need to recruit only one bomber; the world must protect thousands of commercial airports with more than 100,000 daily flights.21

Aviation security has improved, although performance levels, when tested, have sometimes been disappointing. There is public and political pressure to improve effectiveness, reduce inconvenience, and lower costs all at the same time—competing goals that are difficult to achieve simultaneously. Yet, overall, one can assert that the technology has become more effective as well as more efficient in reducing false alarms and inspection delays.

Future passenger screening will increasingly combine information obtained from the moment flight reservations are made to aircraft boarding. Passengers will no longer be required to remove items from their carry-on luggage. Physical screening will not be confined to checkpoints but will also combine new technologies. These gains in efficiency, however, may be offset to some degree by growing passenger loads, especially in areas of the world where resources to acquire the new technology and the training of operators may lag.

Aviation security is also a victim of its own success. As memories of the 9/11 attacks fade, and as there are fewer hijackings or bombings to remind people of the terrorist threat, public complacency will enable those in government who are determined to cut costs to reduce security budgets or to shift them from a national responsibility to a private sector concern. We already see this happening. Many officials still tend to view terrorism as they do war - as a finite undertaking - and to look for an end to the threat and a peace dividend. More than a half-century after the first terrorist hijackings and bombings, this fatigue is understandable, but it is wrong.

### Terrorist Attacks on Surface Transportation

Since terrorists can attack anything, anywhere, anytime, their range of targets is broad and statistically random. To focus on a specific class of targets, therefore, seems arbitrary - like examining terrorist attacks on targets that begin with the letter C. However, the targets selected by terrorist groups are not random from their perspective. Their choices reflect strategies and operational considerations.
As we have seen, terrorist attacks on commercial aviation - in particular, those carried out by Palestinian groups in the late 1960s and early 1970s - reflected the terrorists’ determination to attack Israeli targets abroad because tight security made operations inside Israel difficult. Going after airliners also allowed them to leverage or punish nations that supported Israel, and it fit with their desire to obtain greater publicity and international support for their cause. It was a strategic decision.

Similarly, Al-Qaeda saw attacks on airliners or using hijacked airliners as weapons as a means of achieving the high body counts that would not only cause worldwide alarm but would also bring them publicity, recruits, and financial support. That also was a strategic decision.

The same is true of terrorist attacks on surface transportation targets. The thousands of attacks on trains and train stations, metros, buses, and bus depots since 1970 have been carried out by a diverse group of attackers, including individuals propelled by idiosyncratic causes, which are sometimes hard to discern. Their choice of transportation targets reflects their personal mindsets and operational considerations, but the attackers are also frequently imitating what they have seen in the news media. The choice of certain tactics and targets often follows a contagion pattern - one spectacular event inspires copycats.

If, however, we look at cases where specific terrorist groups have waged campaigns against surface transportation targets, we again see evidence of a strategic and operational logic from their point of view.

A Long History of Rail Sabotage

Targeting rail systems has been a feature of warfare since rail systems became a major mode of transporting goods and people, including troops. During the American Civil War, both sides sabotaged railroads to impede enemy logistics. World War I saw numerous attacks on rail lines and dramatic derailments - for example, attacks by Arab raiders on the Turkish rail line in the Middle East. During World War II, rail yards and rolling stock were targets of strategic bombing, but also targets of resistance fighters in German-occupied Western Europe. The most intensive sabotage campaign took place in German-occupied Russia, where poor roads made German forces heavily dependent on rail systems. As part of what was officially called “the Railway War,” hundreds of attacks were carried out by thousands of Soviet saboteurs operating behind German lines. The Soviet Army trained and equipped them and coordinated their operations.

The partisans used bombs with long-term delays, pressure- or vibration-triggered bombs, and command-detoned devices to destroy gasoline-filled tank cars, as well as magnetic mines with time-delay fuses, all supplied by the Soviet Army.

By 1943, German forces were struggling to deal with more than 1,000 rail sabotage incidents a month. In just two nights in 1944, Soviet partisans cut the rails in 8,422 places. Those running the trains had to remove an additional 2,478 mines. A single night later in the war saw more than 10,000 demolition actions. Partisans also fired anti-tank weapons at locomotives and attacked German rail repair crews. In the second phase of the Railway War, during the autumn of 1943, Soviet partisans destroyed more than 10,000 trains and 72 bridges and caused 30,000 casualties.22

Sabotage of rail lines and attacks on trains have also been a component of civil wars and insurgent campaigns. Rail sabotage and attacks on trains were prominent features of the Spanish Civil War (1936–1939), the Palestinian uprising (1936–1939), the Jewish insurgency (1944–1948), the First Indochina War (1946–1954), the separatist insurgency in southern Thailand (since 1948), Colombia’s Marxist insurgency (since 1962), and the Naxalite insurgency in India (since 1967). Angola’s civil war (1975–2002) destroyed most of the country’s rail infrastructure. Mozambique’s civil war (1977–1992) similarly caused heavy
damage to the country’s rail system. India’s Naxalite insurgents and guerrillas in southern Thailand continue to attack rail systems and passenger trains.

**Terrorists Seek Disruption, Fear, and Increasingly High Body Counts**

Wartime saboteurs concerned themselves with disrupting supply lines and preventing reinforcements from reaching the front. Effective disruption required sustained campaigns, a high volume of attacks, central direction, a large supply of demolition equipment, and large numbers of operatives. Recent insurgencies, in contrast, have sought to disrupt rail traffic as a mode of economic warfare, but also to kill ordinary passengers.

Terrorists today think differently about attacking trains. They are unable to replicate the magnitude of wartime sabotage campaigns and can rarely match the sophistication of those campaigns. Instead, terrorists seek easy targets for less-frequent attacks which are aimed at attracting attention, creating alarm, and causing disruption.

The first generation of urban guerrillas and terrorists in Latin America, Western Europe, North America, and the Middle East focused their attacks on government officials, diplomats, and commercial aviation. For the most part, they did not target surface transportation. The Provisional Wing of the Irish Republican Army (IRA) and the Basque separatist group Euskadi Ta Askatasuna (ETA) were exceptions.

Beginning in the 1980s, terrorist attacks on surface transportation were increasingly intended to cause mass casualties. The terrorists targeted passenger trains and stations and rarely went after infrastructure. While derailing speeding passenger trains remains a terrorist dream - and in some cases, the terrorists have succeeded - their more frequent targets have been metro systems and commuter trains, where high volumes of passengers offer opportunities for high body counts. By the late 20th century, bombings in train stations or on trains had become one of the most common terrorist tactics.

**The IRA Campaign against Transport in England**

The IRA was one of the first groups to initiate a bombing campaign targeting British rail passengers. For the first few years of its armed struggle, the IRA confined its terrorist operations to Northern Ireland, but in 1973, the group “exported” its campaign to England and began carrying out bombings in London. This fit with the IRA’s overall strategy to impose a high psychological and economic burden on the British public and its government as a price for remaining in Northern Ireland. “Active Service Units” - clandestine cells of IRA bombers - initially targeted government buildings but later expanded their targets to include hotels, restaurants, and tourist sites, as well as train and Tube stations.

Many of the IRA attacks caused injuries and some caused fatalities, but the IRA was cautious. It had the capability to cause mass casualties -its members knew how to make bombs. But unlike the generation of jihadist terrorists that operated in the UK decades later, the IRA operated within self-imposed constraints. Its goal was to levy an unacceptable cost on Britain until its leaders decided it was no longer worth remaining in Northern Ireland - a strategy drawn from earlier anti-colonial contests. Massacres might repel the IRA’s own supporters and reduce financial contributions from sympathizers abroad.

As a precaution, the IRA often provided authorities with warnings of where and when bombs were about to go off, claiming that it did so in order to give them time to evacuate the area and avoid casualties. Providing “warnings” offered the group cover when people were killed by IRA bombs, allowing it to shift culpability to the authorities, but warnings were not always given, the information was not always precise, and sometimes it was misleading.
Warnings were timed to force the authorities to evacuate large facilities quickly, creating potential panics, giving them just enough time to respond but not enough time to search. The IRA also called in hoax warnings to increase disruption. IRA operatives might plant one bomb to establish credibility while claiming to have planted many more, none of which targets could be ignored.

As an example, the IRA set off a bomb in London’s Paddington Station at dawn on 18 February 1991. The station was empty, and the explosion injured no one, but it established credibility for a subsequent IRA call, warning that bombs would explode at all 11 of the main-line train stations in London during the morning rush hour. An evacuation of this magnitude was unprecedented, and the police hesitated before halting all incoming trains and evacuating every station, which would have put thousands of people into the streets. It would be a dangerous course of action that would put crowds of people in harm’s way if the streets were where the IRA actually had planted bombs - and in some cases, the terrorists did plant secondary devices aimed at killing arriving police and others who gathered at the scene of an explosion.

Before ordering a massive evacuation, the authorities tried to search the stations. As a result, passengers were still present on a crowded platform when a bomb hidden in a trash can went off in Victoria Station five minutes before the detonation time given in the warning. The explosion killed one person and injured 38. Fearing further casualties, the authorities shut down all of the other train stations for the first time in history.

The ETA Campaign against Spanish Railways

Spain’s Basque separatist ETA was a contemporary of the IRA. Beginning in the late 1960s, it carried out a campaign of assassinations, armed assaults, and bombings directed against Spanish government officials, Spain’s security forces, and civilian targets, including Spain’s rail system. ETA claimed responsibility for, or was directly linked to, 25 attacks on transportation targets; another 77 unclaimed attacks were also attributed to it.

ETA was even more cautious than the IRA about civilian casualties. Its attacks on transportation targets were intended to demonstrate its capabilities, cause fear and disruption, and discourage tourism as part of its campaign of economic warfare. Most of its attacks targeted empty trains and stations. When ETA planted bombs where civilian bystanders were likely to be killed, it - like the IRA - provided warnings. Only two of its many attacks on rail targets resulted in fatalities: four people were killed by bombs detonated in the Atocha and Chamartin train stations in Madrid on 29 July 1979.

However, as is the case in many terrorist campaigns, there was pressure to escalate the violence. In 2003, Spanish police thwarted an ETA plot to detonate two suitcases containing bombs with more than 50 kilos of explosives on a train in Madrid’s Chamartin train station on Christmas Eve. The arrest and interrogation of the individual attempting to plant one bomb alerted police to the second bomb, which was already on its way to Madrid. Authorities halted the Madrid-bound train, evacuated its passengers, and defused the device. On 29 February 2004, police arrested two ETA members driving vans carrying 536 kilos of explosives on their way to Madrid. The arrest interrupted a terrorist plan to detonate a massive vehicle bomb there on the day of the national elections, scheduled for 14 March.

It is understandable, therefore, that ETA would be at the top of the list of suspects when ten bombs went off on four commuter trains arriving at Madrid’s Atocha rail station on 11 March 2004, killing 193 people and injuring around 2000 others. However, police quickly realized that the design of the devices and the explosives used were different from devices fabricated by ETA. This and other evidence convinced police that the bombs were the work of jihadists, not Basque separatists.
Spanish police were therefore surprised when the Minister of Interior announced that ETA was responsible, a claim that Spanish political leaders persisted in making despite overwhelming evidence to the contrary. This infuriated many people, who considered the government’s claim as an attempt to cover up what people saw as a terrorist attack in retaliation for Spain joining the US in the invasion of Iraq.

A detailed analysis of the March 11 bombing by Fernando Reinares makes the point that both sides were wrong: ETA was not responsible for the attack, despite continuing conspiracy theories; and the decision by jihadists to carry out a major terrorist attack in Spain was already made in December 2001. The jihadist network in Spain that carried out the attack assembled in March 2002, and Al-Qaeda’s senior leadership approved the plan in October 2003, all long before Spain joined the American-led coalition to invade Iraq.25

Transportation targets were not a feature in the terrorist campaigns of Germany’s Red Army Faction, Italy’s Red Brigades terrorists in the 1970s and 1980s, or other groups active during the period. Neo-fascists, however, bombed an express train in Italy in 1974, killing 12 people and injuring 48, and they bombed the Bologna Central railway station in 1980, killing 80 people and injuring more than 200 others. The Sicilian Mafia was believed responsible for the bombing of a passenger train in 1984 that killed 16 and injured 256.

The Tokyo Sarin Attack

The terrorist events described above were exceptions and reflected different mindsets and motives. Terrorist violence in general, however, escalated during the 1980s and 1990s, prompting fears that terrorists would eventually resort to using weapons of mass destruction - chemical, biological, radiological, or nuclear (CBRN) weapons. A survey of terrorism experts in 1985 indicated that most thought the use of nuclear weapons was highly unlikely, while some thought that terrorists might try to use some form of biological weapons. A majority thought it likely that terrorists would use chemical weapons before the end of the century.26 Their guess was right.

On 20 March 1995, members of Aum Shinrikyo, an apocalyptic Japanese cult, dropped and punctured plastic bags filled with sarin, a lethal nerve agent, on five Tokyo subway trains as they reached the central part of the city, where government buildings were concentrated. As the quality of the sarin manufactured by the group was poor and the method of dispersal was primitive, only 12 persons died in the attack, although more than 1,000 people were directly exposed to the fumes, and more than 5,500 were treated for a variety of medical conditions related to the attack. Had the sarin been more potent and the dispersal more effective, the number of deaths would have been much higher.27

Weeks later, Aum Shinrikyo members still at large attempted another attack on Tokyo’s subway system, this time using hydrogen cyanide. The dispersal scheme did not work as planned, although four people were injured. With these incidents, chemical weapons had become part of the threat matrix, but they did not initiate a trend, although Al-Qaeda operatives later plotted attacks involving lethal chemicals and biological substances. Old-fashioned bombings and derailments continued to account for the highest-casualty attacks.

Campaigns Against Railways Continue

In July 1995, a small group of Algerian extremists, angered by France’s support of the Algerian government in its war against Islamists, detonated a bomb aboard a French commuter train at the St. Michel station in Paris. Seven persons died in the explosion, and more than 80 were injured. This was the first of a series of attacks, several of which were directed against transportation targets, that continued until mid-October. In August, the terrorists
unsuccessfully attempted to derail a high-speed train between Lyon and Paris. In October, a bomb exploded on a commuter train in Paris, injuring 30 people. After a long hiatus, when the campaign appeared to have ended, another bomb exploded on a commuter train in Paris in December 1996, killing four persons and injuring more than 90 others.\(^{28}\)

India has experienced more attacks on surface transportation than any other country and has suffered some of the deadliest incidents. Terrorist attacks on commuter and intercity passenger trains in India became increasingly common in the first years of the 21st century. In 2002, sabotage caused the derailment of a high-speed passenger train crossing a bridge, resulting in between 130 and 200 fatalities. The incident was blamed on Naxalite or Maoist guerrillas, who are responsible for many of the attacks on Indian trains. Another derailment caused by Maoists in 2010 killed more than 90 persons. In addition to Maoist rebels, separatists in northeastern India and jihadist extremists, including operatives of the Islamic State, have also attacked India’s trains.

**Attacks on Buses**

While the IRA and ETA usually targeted trains, other groups went after buses and bus depots. The choice appears to have been operationally determined. For terrorists bent upon mass casualties, train attacks offer higher body counts, since speeding passenger trains can be derailed, trains and train stations can be attacked with multiple explosive devices, and train targets include packed metros and subways. Only a limited number of people can be killed on a single bus. However, buses are the primary form of public transportation in many developing countries and also in Israel.

Terrorist attacks on buses increased during the Palestinian uprising known as the Intifada (1987–1993), but the Second Intifada (2000–2006) may have been the most intensive and lethal campaign waged in any country, with the possible exception of Sri Lanka’s civil war, which lasted from 1983 to 2009. According to Israeli statistics, Palestinian organizations during the Second Intifada carried out thousands of attacks between 29 September 2000, and the end of 2005. Although many of these had negligible results, 1,084 Israelis were killed, and more than 6,000 others were injured.\(^{29}\)

Bombings of buses and bus depots have been common in conflict zones across much of Africa and South Asia. They also have been a feature of jihadist campaigns in the Middle East.

Only 147 of the recorded attacks on buses were suicide attacks, but they caused 49 percent of the fatalities and 56 percent of the injuries. Suicide bombings of urban buses, which are small confined environments, made ideal targets for suicide bombers and buses in Tel Aviv and Haifa and figure prominently among the high-casualty events. Buses ripped apart, with bodies strewn across the streets, created horrific images that added to the alarm.\(^{30}\)

**The Jihadist Threat to Surface Transport**

Fanatics inspired by Islamist ideology have posed the greatest threat to surface transportation targets in first two decades of this century. An analysis of jihadist targeting preferences in Europe between 1996 and 2016 showed that transportation (aviation and surface) was the most frequent intended target in jihadist plots, ahead of public areas in general.\(^{31}\)

The attacks on transportation are part of a global terrorist campaign initially inspired by continuing exhortations from Al-Qaeda leader Osama bin Laden and other Al-Qaeda communicators. Al-Qaeda’s rival, the Islamic State of Iraq and Syria (ISIS), which emerged during Syria’s civil war, has also attacked transportation targets, including a Russian airliner sabotaged in Egypt in 2015.
In contrast to the 9/11 hijackings, the attacks on surface transportation targets have been carried out by home-grown terrorists, although some of them received instruction in training camps run by Al-Qaeda or ISIS or had learned from information posted on jihadist websites. The jihadists in all cases sought to inflict mass casualties - the objective was carnage, not disruption. Transportation venues became killing fields.

The 2004 bombing attack on Madrid’s commuter trains has already been mentioned. The following year, suicide bombers attacked London’s underground, and one device was detonated aboard a London bus. In total, fifty-two persons were killed, and hundreds were injured. Two weeks later, four jihadist bombers attempted to replicate the attack, but their devices were faulty.

In 2006, jihadists in India planted bombs aboard a Mumbai commuter train, killing 209 persons. In 2007, bombs hidden in the coaches of a passenger train killed another 70 persons.

The Chechen insurgency in Russia started out as an independence movement, but over time it acquired a more radical jihadist ideology. Between 2003 and 2017, Chechen rebels/Islamists carried on a deadly bombing campaign targeting passenger trains and stations and urban metros in Moscow and other cities in Russia.

In 2004, a suicide attacker detonated a device on Moscow’s packed metro during the rush hour, killing 40 people and injuring more than 100 others (later that year, as noted above, two female suicide bombers brought down two Russian airliners, killing 88 persons). In 2010, two blasts in Moscow metro stations killed 40 people. On December 29 and 30 of that year, two suicide bombers carried out attacks at Volgograd’s train station and on a trolleybus, killing a total of 30 persons. In all, jihadist attacks on surface transportation in Russia killed more than 240 people and wounded hundreds more.

**Derailments: A Terrorist Dream**

While bombings aboard packed trains or in crowded stations offered jihadists the high body counts they wanted, speeding passenger trains crashing into ravines promised the spectacular images terrorists dreamed about. After 9/11, derailing trains became an obsession. Computer files recovered during the 2011 raid on Osama bin Laden’s hideout in Pakistan indicate that at the time of his death, Al-Qaeda was looking for ways to “celebrate” the tenth anniversary of 9/11 by carrying out a major terrorist attack in the US. This would show that the Al-Qaeda enterprise was still in business ten years later. Bin Laden’s proposed plan was to derail a passenger train as it crossed a high bridge, plunging the coaches into a river or deep valley, killing hundreds.

The Mineta Transportation Institute database includes 17 attempts by jihadists to sabotage rails, including 10 definite attempts to derail trains. Although other categories of attackers have carried out more-frequent attacks, the jihadist operations were by far the deadliest attacks.32

Saboteurs in 2007 detonated a bomb under the tracks of the Moscow-St. Petersburg Express to derail it as it passed over a bridge. The train managed to clear the bridge before the coaches derailed, and instead of plunging down the steep slope as anticipated, the coaches slid on their sides. Scores of people were injured, some seriously, but there were no fatalities. Saboteurs struck the same line again in 2009, and this time they succeeded in causing a deadly derailment - 26 people were killed, 97 injured. In both cases, Islamist fanatics from Ingushetia in Russia’s turbulent North Caucasus were identified as the perpetrators. In 2011, Russian authorities foiled another attempt to sabotage the Moscow-St. Petersburg train.

In 2016, saboteurs derailed 14 coaches of the Indore-Patna Express in India’s Uttar Pradesh state, killing 148 people and injuring 125 others. Initially, the derailment was thought to have been caused by a mechanical problem, but Indian authorities later blamed an ISIS cell operating in the area.
In 2017, ISIS supporters from Tajikistan attempted to sabotage a high-speed train, causing it to derail in the path of another train traveling in the opposite direction. The trains did not crash, and there were no casualties, but the coaches sustained extensive damage.

These incidents show that derailments can be deadly but are difficult to carry out. Surface transportation offers easier, less spectacular but still deadly ways of attacking. Police uncovered several jihadist plots against French rail targets in the early 2000s, and a 2015 attempt to gun down passengers on the high-speed train between Amsterdam and Paris was foiled by passengers. Members of the same network of Belgian and French ISIS recruits carried out coordinated bombings at the Brussels airport and on the Brussels metro in 2016, killing a total of 32 people. Police shot and killed another bomber at the Brussels Central Train Station in 2017.

**Recent Terrorist Plots indicate a Continuing Threat**

In addition to the jihadist attacks on surface transportation that have occurred, police have uncovered numerous jihadist plots. British authorities uncovered plans to disperse poison gas and ricin on London trains in 2002 and 2003. In 2003, jihadists also planned to release cyanide gas in New York’s subway system but reportedly were diverted to another project. Authorities thwarted a plot by homegrown jihadists to bomb a subway station in midtown Manhattan in 2004. In November 2005, Australian authorities uncovered a plot to carry out attacks in Sydney and Melbourne; targets included Melbourne’s landmark Flinders Street Rail Station.

In 2006, homegrown jihadists planned to detonate two bombs hidden in suitcases on German commuter trains, but the devices failed to detonate. That same year, Lebanese authorities discovered another jihadist plot to bomb trains in the tunnel under the Hudson River, and Moroccan police uncovered a jihadist plot to bomb Milan’s metro in Italy.

In 2008, police in Spain uncovered a jihadist plot to carry out bombings on Barcelona’s metro. An American jihadist who traveled to Pakistan offered his experience as a former employee of the Long Island Railroad to help Al-Qaeda plan and execute a terrorist attack on that system. He was arrested by Pakistani authorities and returned to the US.

The following year, acting on a tip from British authorities, FBI agents uncovered the existence of a group of jihadists planning to carry out suicide bombings on New York’s subways. Another individual was arrested the following year in an undercover operation. He intended to carry out a bombing on the Washington DC metro. Even if most of the plots were aspirational, they indicate that attacks on transportation targets remain in terrorist playbooks.

**Trends in Tactics**

Thus far, we have been looking at terrorist attacks on surface transportation historically, by group and country. In this section, we look at the broader trends in terrorist tactics regarding attacks on transportation.

Terrorist attacks on surface transportation targets have increased over the long run. Between 1970 and 1979, terrorists carried out a total of 23 surface transportation attacks that caused fatalities (only incidents with fatalities are included in this analysis to mitigate apparent increases that may be due solely to better reporting.). The number grew to 44 attacks with fatalities in the 1980s, 271 in the 1990s, 446 in the decade between 2000 and 2009, and 814 in the decade between 2010 and (15 October) 2019. These numbers include attacks on both bus and passenger rail targets.

Most of the attacks on surface transportation involved few or no fatalities, but 11 of them since 9/11 resulted in 50 or more deaths, and three of these killed nearly or slightly more than 200 people each. The total number of fatalities in these 14 attacks would translate into the
casualties from roughly 12 or 13 commercial airline crashes.\textsuperscript{35} One can imagine the fear and furor that would have resulted if 13 commercial airliners had been brought down by terrorists since 9/11.

The total number of fatalities caused by attacks on surface transportation also increased, although both the number of incidents and the number of fatalities declined sharply after 2015. Overall lethality - the average number of fatalities per attack - appears to have declined slightly over the years, but this is due to a few high-casualty events in the 1970s and 1980s combined with a lower number of total events in those years, resulting in a higher average fatality per attack and tipping the trend line downward. If these few incidents are set aside, the trend line tips slightly upward. The greater number of high-fatality events in recent years is offset by the growing volume of low-level attacks, which lowers the average lethality rate. We also cannot dismiss the possibility that some portion of the increased volume of incidents recorded in recent years may be due simply to better reporting as more local news accounts become available via the internet.

Bombings account for most of the attacks on surface transportation and most of the casualties. Improvised explosive devices (IEDs), grenades, and mines were used in about 60 percent of the attacks. Bombings are also the most lethal form of attack. Shootings and armed assaults constitute 15 percent of the attacks. Incendiary devices and other forms of arson account for nearly 13 percent of all attacks, and mechanical means of sabotage (mostly of rails) account for about three percent.\textsuperscript{36}

Recently, there has been an increase in more-primitive terrorist tactics - stabbings and vehicle-ramming attacks. There have also been incidents in which people are pushed off platforms into oncoming trains. The trend reflects changes in how terrorists are recruited. In the past, terrorists usually joined small underground groups that carefully vetted them to prevent infiltrators or individuals judged to be unreliable. In contrast, much of today’s terrorist recruiting is done by exhortation. Jihadist groups, in particular, have exploited the Internet and social media to inspire followers abroad to carry out attacks wherever they are, using whatever means they have available. Often operating alone, the recruited individuals have limited resources and skills. Guns, where they are easily available, may be used. Knives and vehicles are readily accessible almost everywhere.\textsuperscript{37}

Remote recruiting emphasizes the violence of attacks as much as the causes for which they are carried out, and it appeals to a broader audience of potential actors that includes not only fanatics, but individuals with histories of aggression and violence, as well as mentally disturbed persons. Intense media coverage adds to the attraction. The result is an increase in random attacks by individuals untethered to organizations.

\textit{An Aviation Security Model won’t work for Surface Transportation Attack Prevention}

Although the immediate threat posed by Al-Qaeda and ISIS appears to have diminished, it must be presumed that the threat will continue, because individual jihadists or operatives of other groups will view surface transportation as a target if only because it offers high body counts in easily accessible venues. Security measures for surface transportation cannot replicate those in place for aviation security. To begin with, the volume of passengers using public surface transportation greatly exceeds that of airline passengers. Rigorous passenger screening would require a vast army of security personnel.

Train stations, especially metro stations, are configured to allow as many people as possible access from multiple points. They do not lend themselves to security checkpoints, which could create long lines of waiting passengers who would be vulnerable to attack. Moreover, delay times for security that may be acceptable to passengers boarding flights would be inconvenient if imposed twice daily on commuters - especially during rush hours. While the costs of security represent a small portion of an airline ticket, adding them to the cost of commuter travel could
render public surface transportation unaffordable for many. In the future, new technology may allow effective, low-cost inspection that still allows rapid, high-volume passage, but for the foreseeable future, attempts to replicate the aviation model will not work.

There is one further consideration. Security measures should offer a “net security benefit,” that is, the security measures cannot easily be obviated by merely shifting targets. The argument for a net security benefit can be made in the case of aviation, where a bomb can bring down an airliner, causing hundreds of fatalities, or hijacked airliners can be turned into missiles killing thousands. Public surface transportation offers crowds, but so do many other accessible venues. Keeping bombers and shooters off trains and out of train stations and bus depots is desirable, but the net benefit to society is less (there are some exceptions, such as preventing explosions in deep tunnels where the destructive effects are magnified and rescues are difficult).38

The argument can be made that terrorist attacks on surface transportation have a greater psychological effect than, say, terrorist attacks on night clubs or movie theaters, even though the casualties may be the same, and therefore such attacks have greater economic consequences. Higher security for surface transportation, therefore, may be justified.

Security for surface transportation differs from aviation security in one further aspect. Today’s aviation security is multilayered, beginning the moment one makes reservations for air travel and extending through security checkpoints and air marshals and armored cockpit doors, not to mention alarmed passengers who are no longer passive bystanders in threatening situations. But while it has layers of defense, aviation security is still front-loaded, that is, it concentrates resources on preventing weapons or explosives from getting on airplanes. Once a bomb goes off, there is little that can be done to mitigate the consequences.

In contrast to airline transportation, public surface transportation does not allow many opportunities for prevention. Except for longer trips by rail that require reservations, there are fewer opportunities to confirm identities or check them against terrorism databases. And, as already mentioned, with some exceptions, there are fewer opportunities for security checkpoints at boarding places. However, there are greater opportunities for immediate intervention in the event of an attack, for prompt evacuation out of harm’s way, and for rapid rescue, all of which may mitigate casualties. Public surface transportation security, therefore, can be addressed with broader strategies and along a lengthier timeline. It begins with station design and construction, which can facilitate surveillance and mitigate casualties by creating large open spaces rather than confined environments. Design and construction measures can also eliminate those things (such as glass) that can turn into shrapnel or burn with toxic fumes and can facilitate rapid evacuation and rescue. The same principles apply to bus design.

CCTV is already widely used in surface transportation systems. Software is making CCTV systems smarter and capable of learning and recognizing anomalous behavior. Although it is more controversial from a civil liberties perspective, facial recognition technology is developing rapidly and increasingly being deployed.

Behavioral detection is another controversial security measure. The science is still debated, and its application can easily turn into racial or ethnic profiling, but it is already a standard component of many airports and may be used more widely in surface transportation security.

Police presence, which anecdotal information indicates has some deterrent effect, can be increased or deployed in accordance with threat information or on a random basis. A more limited form of passenger screening is in place for some commuter systems that conduct random passenger screening. This allows the operators to design and test screening protocols and train security personnel. Based upon threat conditions, the screening can be quickly expanded if necessary and can just as quickly be reduced.39 Screening can be accompanied by behavioral detection. Explosives detection - primarily by canine units - is widely used. Dogs are now trained to follow vapor trails instead of sniffing individual objects.40
Enlisting public participation in “See Something – Say Something” campaigns appears promising. While crowded stations and coaches may seem chaotic to an observer, they are familiar territory to regular commuters, who are often able to spot things that are out of order. Staff training adds eyes and ears to the security effort. According to a statistical analysis done by the Mineta Transportation Institute, transport staff and passengers play an important role in the prevention of terrorist attacks. “By discovering and reporting suspicious objects, they have prevented more than 10 percent of all terrorist attacks on public surface transportation. Detection rates are even better in the economically advanced countries where more than 14 percent of the attempts are detected - and have been improving.”

Aviation security, like aviation safety, is government regulated, reflecting a long tradition and the necessity of applying the same rules across the entire system. A new mode of attack anywhere is viewed as a potential global threat. In most cases, surface transportation security remains the responsibility of the operators and local authorities. Attackers are mostly local. Although an individual anywhere may carry out an attack, threat levels vary by country and city.

Instead of a regulatory approach, public surface transportation operates on a “best-practices” mode. Threats are assessed by central government authorities and local police. Attacks are analyzed for lessons learned. Information is shared with local authorities and operators, who then make individual decisions about the level and nature of security appropriate to their situation rather than conforming to a regulatory regime. The central government conducts research and may add resources in the form of personnel for security duties or financial support, although in countries where authority is traditionally more centralized and the threat level is high, central government intervention and control may increase.

Security does not come cheap, and surface transportation operators are under public and political pressure to keep fares low. This places low ceilings on security expenditures and creates a need for government subsidy. Some governments have reacted by treating public transportation - both air and ground - as a matter of national security. Others offer security assistance but leave funding and decision-making to the operators. As a result, surface transportation security remains a patchwork quilt with great variations.

**How Much Security is Enough?**

There is, of course, the fundamental question: how much security is enough? This is not easily answered in dealing with events that have low probability but potentially high consequences. The nature of the terrorist threat makes it even more difficult to answer.

As noted earlier, terrorists can attack almost anything, anywhere, anytime, while we cannot protect everything, everywhere, all the time. That gives the terrorists a tremendous advantage, enabling them to obviate security measures by merely shifting their sights. It also means that consequences must be measured in terms of psychological effects, as well as casualties and physical destruction.

Accurate statistics about terrorism are extremely difficult to compile. Differences in definitions of terrorism, criteria for collection, and limitations on collection capabilities mean that no two sets of numbers agree, and data are often incomplete. Nevertheless, combining the Mineta Transportation Institute’s database of attacks on surface transportation systems, which includes nearly 50 years of information and has been an ongoing enterprise for the past 25 years, with a proprietary database of attacks on commercial aviation being compiled by Bruce R. Butterworth gives us a fairly good estimate of the total number of events and casualties.

The aviation database includes 1,123 events with 6,196 fatalities that occurred between 1970 and the end of 2019. The events include airline hijackings, airline sabotage, and attacks on airports (for all but 15 years) and aircraft on the ground. The data exclude apparent suicides.
by commercial pilots who deliberately crashed their airplanes, killing all on board; attacks on airline ticket offices, navigational aids, and other infrastructure; and military activity in war zones. Spread over 50 years, the average annual total number of deaths from attacks on commercial aviation worldwide is 124. As the database is refined, these figures will shift somewhat, but not significantly.

If the 2,977 persons who died as a result of the 9/11 attacks are excluded, this gives us a rough average of three fatalities per attack.

There were a total number of 4,182 attacks against buses, bus depots, passenger trains (including metros and subways), train stations, and passenger ferries and terminals between 1970 and the end of 2019. The attacks resulted in 12,052 fatalities, producing a rough average of three fatalities per attack and an annual average of 241 fatalities worldwide.

At the risk of sounding callous about thousands of individual tragedies, these are not huge numbers. A strict application of cost-benefit analysis of security measures in place to prevent attacks on transportation targets, especially commercial aviation, would challenge the expenditures. Taken together, the total worldwide volume of deaths is roughly equivalent to the annual homicide toll in the US alone. We know that hundreds of thousands of people are murdered in the world every year, and more than a million die annually in automobile accidents.

Including economic damage and disruption in the tally alters the calculations. Major terrorist attacks produce cascading economic consequences, but do these suffice to merit the billions of dollars spent over the years on prevention?

The problem is that terrorist attacks, which are intended to create alarm, have enormous psychological impact, which cannot be ignored. We know that single deaths, although high in volume, have less psychological effect than incidents with multiple fatalities. The psychological effect of a plane crash that kills 100 people at once is far greater than the effect of hundred individual deaths from other causes. Psychologically, its effects may be closer to an event of 10,000 fatalities, although the effects will vary greatly according to the society and the circumstances.

An event that involves deliberate mayhem has a greater psychological effect than accidental deaths. Attacks that take place closer to home have a greater effect than faraway attacks. Even the primitive terrorist stabbing attacks that have become more frequent in recent years create the impression that nowhere is one safe, thereby adding to the level of anxiety.

Fear can have insidious but real effects on the economy; it can create political crises that bring down governments; it can exacerbate other anxieties; it can provoke rage that leads to war. While cantankerous passengers may complain about taking their shoes off at airports or being selected for a random check before entering a subway station, the public demands security or head will roll when a terrorist attack is not prevented.

Societies subjected to continuing terrorist campaigns may come to accept terrorism as a fact of life, but over time, attitudes change. Suppressed fear hardens into hatred. Tolerance declines. Democracy itself is imperiled. A state of security gradually becomes a security state.

Brian Michael Jenkins holds academic degrees from the University of California at Los Angeles. He also studied at the University of Guanajuato, Mexico, and at the University of San Carlos, Guatemala. Commissioned in the Army at the age of 19, Mr. Jenkins became a paratrooper and captain in the Green Berets. He served in the 7th Special Forces Group in the Dominican Republic and later as a member of the 5th Special Forces Group in Vietnam (1966–1967). He returned to Vietnam in 1968 to serve as a member of the Long Range Planning Task Group. In 1989, Mr. Jenkins served as an advisor to the national commission established to review terrorist threats following the bombing of Pan Am 103. Following the 1993 bombing of the World Trade Center, he served as a member of the team assembled to
review threats and develop new security measures. In 1996, President Clinton appointed Mr. Jenkins to the White House Commission on Aviation Safety and Security. From 1999 to 2000, he served as an advisor to the National Commission on Terrorism. Mr. Jenkins is the Senior Adviser to the President of the RAND Corporation and also the Director of the National Transportation Security Center at the Mineta Transportation Institute. B.M. Jenkins is the author of “International Terrorism: A New Mode of Conflict”; the editor and co-author of “Terrorism and Personal Protection”; the co-editor and co-author of “Aviation Terrorism and Security”. His other books include “Unconquerable Nation” and “Will Terrorists Go Nuclear?”
Endnotes

1 Green, David B. ‘This Day in Jewish History/The First and Only El Al Hijacking’, *Haaretz*, 23 July 2013. Available at: haaretz.com/jewish/premium-this-day-the-first-and-only-el-al-hijacking-1.5298481.


8 Wilkinson and Jenkins 1998.


10 Ibid.


15 Although details of this plot are in public records of the World Trade Center bombing trial, both the 9/11 Congressional Inquiry and the 9/11 Commission Report fail to mention it. History Commons, ‘Complete 911 Timeline: Sheikh Omar Abdul-Rahman’. Available at: http://www.historycommons.org/timeline.jsp?timeline=complete_911_timeline&other_al-qaeda_operatives=complete_911_timeline_sheikh_omar_abdul_rahman .

16 The “Red Team” created to examine potential threats to the World Trade Center following the 1993 bombing postulated a plane crashing into the towers as a possible scenario. The author of this chapter directed the threat analysis.


18 These statistics derive from a database compiled by Bruce R. Butterworth, the former Director of Aviation Security Operations at the US Federal Aviation Administration.


For a more detailed account of the IRA campaign against British transport, see: Jenkins, Brian Michael and Larry N. Gersten, Protecting Surface Transportation Systems and Patrons from Terrorist Activities, San Jose, CA: Mineta Transportation Institute, 2001.


The results of the survey appeared in Jenkins, Brian Michael (ed.), TVI [Terrorism, Violence, and Insurgency] Journal, 1985. Readers, who were mostly law enforcement, military, and others concerned with terrorism, as well as private security personnel and researchers, were asked to assess the probability that terrorists would employ chemical, biological, or nuclear weapons by the end of the century. Respondents considered only chemical weapons more likely than not to be used. The survey, of course, had no scientific value - it was merely a quantification of guesses.


Butterworth, Doley, and Jenkins (2012).


Jenkins, Brian Michael, and Bruce R. Butterworth, Train Wrecks and Track Attacks: An Analysis of Attempts by Terrorists and Other Extremists to Derail Trains or Disrupt Rail Transportation, San Jose, CA: Mineta Transportation Institute, 2018. Available at: https://transweb.sjsu.edu/research/1794-Train-Wreck-Train-Attacks.

Various terrorist plots against transportation targets are examined in: Jenkins, Brian Michael and Joseph Trella, Carnage Interrupted: An Analysis of Fifteen Terrorist Plots Against Public Surface Transportation, San Jose, CA: Mineta Transportation Institute, 2012.
Available at: https://transweb.sjsu.edu/research/carnage-interrupted-analysis-fifteen-terrorist-plots-against-public-surface-transportation.

34 These statistics were provided by the Mineta Transportation Institute database.

35 The average number of fatalities in the four airline crashes caused by terrorist sabotage since 9/11 is 106.5, which gives us a rough equivalent of fatalities in 13 crashes.


37 Jenkins, Brian Michael, and Bruce R. Butterworth, “Smashing into Crowds”- An Analysis of Vehicle Ramming Attacks, San Jose, CA: Mineta Transportation Institute, 2019. Available at: https://transweb.sjsu.edu/research/SP1119-Vehicle-Ramming-Update; see also: Jenkins, Brian Michael, Bruce R. Butterworth, Jean-François Clair, and Joseph Trella III, An Exploration of Transportation Terrorist Stabbing Attacks, San Jose, CA: Mineta Transportation Institute, 2019. Available at: https://transweb.sjsu.edu/research/SP0319-Terrorist-Stabbing-Attacks-Public-Transportation.


41 Jenkins, Brian Michael, and Bruce R. Butterworth, Does “See Something, Say Something” Work? San Jose, CA: Mineta Transportation Institute, 2018. Available at: https://transweb.sjsu.edu/research/SP1118-See-Something-Say-Something. 
Bibliography


Jenkins, Brian Michael, and Bruce R. Butterworth, Selective Screening of Rail Passengers. San Jose, CA: Mineta Transportation Institute, 2007. Available at: https://transweb.sjsu.edu/research/selective-screening-rail-passengers


Jenkins, Brian Michael, and Bruce R. Butterworth, Train Wrecks and Track Attacks: An Analysis of Attempts by Terrorists and Other Extremists to Derail Trains or Disrupt Rail Transportation, San Jose, CA: Mineta Transportation Institute, 2018. Available at: https://transweb.sjsu.edu/research/1794-Train-Wreck-Train-Attacks

Jenkins, Brian Michael, and Bruce R. Butterworth, How Sophisticated Are Terrorist Attacks on Passenger Rail Transportation? Available at: https://transweb.sjsu.edu/research/SP0520-Terrorist-Attacks-Passenger-Rail-Transportation


Web-based Resources

Mineta Transportation Institute, Available at: https://transweb.sjsu.edu/
International Air Transport Association (IATA). Available at: https://www.iata.org/
International Union of Railways (UIC). Available at: https://uic.org/
Chapter 27

Layers of Preventive Measures for Soft Target Protection against Terrorist Attacks

Alex P. Schmid

The chapter opens by listing the most frequently hit soft and hard targets, with a focus on those attacked by jihadi terrorists. This is followed by a conceptual discussion about various types of terrorist targets, both physical and psychological (targets of violence, targets of terror, target of demands and targets of attention) and identifies ten audiences/conflict parties, terrorists aim to influence in one way or another. A survey of a number of empirical studies on terrorist targeting follows, and ten criteria underlying terrorists’ physical target selection are identified. A trend towards increased attacks on soft targets, especially by single actors, is noticed. As a consequence, the number of attacks that could not be prevented has increased in recent years. This diagnostic part of the chapter is followed by one that focuses on improving the prevention of attacks against soft targets. A typology of preventive measures is presented, distinguishing between up-, mid- and downstream prevention. Subsequently, the main focus is on mid- and downstream prevention. A layered approach of combining 13 preventive measures (LPM) is suggested and the author’s proposals are juxtaposed with the 13 Good Practices (GP) proposed by the Global Forum on Counter-Terrorism (GFCT)’s Soft Target Protection Initiative in 2017. There is also an Appendix with “Twelve Rules for Preventing and Countering Terrorism” developed by the author when he was Officer-in-Charge of the Terrorism Prevention Branch of UNODC. A bibliography of new literature on terrorist targeting concludes the chapter.

Keywords: prevention, soft targets, terrorist targeting, religious terrorism, jihadism
For an act of terrorism to occur, you need a motivated perpetrator, a suitable target, and the absence of capable guardians. Soft targets have, by definition, no or few guardians present, and there are plenty of ill- or un-defended crowded places that highly-motivated terrorists find suitable. What can be done in terms of preventing terrorist attacks on targets that are not hardened?

Prevention presupposes that we can forecast, with a high degree of probability, what is likely to happen in the near future and - if it is something harmful - anticipating it, stopping it proactively in time from happening by intervening into the chain linking causes and effects. Preferably, this is to be done as early, upstream, and close to the source as possible. An important tool for predicting terrorist activity is analysing and learning from past events. In other words, if you want to be a futurologist, it helps if you are a historian as well. However, when it comes to terrorism, there are a few new things under the sun. In the past, the prototypical terrorist was a bomber without an air force; this has changed drastically, the 9/11 terrorists used hijacked passenger planes as guided cruise missiles, and today terrorists are turning commercial and homemade drones into a makeshift miniature air force.

**Terminology**

The prevention of terrorism is the pre-attack part of counterterrorism. Some analysts distinguish between anti-terrorism – preventive and defensive measures against terrorism such as target hardening and enhanced patrolling – and the broader concept of counterterrorism that includes also active and offensive (both pre-emptive and retaliatory) efforts to prevent, deter, and combat politically motivated violence directed at civilian and non-combatant targets. In doing so, counterterrorism actors utilize a broad spectrum of responsive measures, such as law enforcement, political, psychological, social, economic and (para-)military measures. For the *Handbook of Terrorism Prevention and Preparedness*, the editor developed the following working definitions:

“Prevention of terrorism involves the anticipation of risks factors giving rise to terrorist group formation, terrorist campaign initiation and/or specific attack preparations,

and responding to these by

Preparedness, that is, taking proactive and pre-emptive measures to reduce risks and threats and, if that turns out to be insufficient, reduce the negative impact of terrorist attacks through a set of planned precautionary measures aimed at strengthening governmental readiness and societal resilience.”

This chapter focuses on the prevention of terrorist attacks on soft targets. Yet, first we have to be clear about terminology. What are “terrorist targets” and, more importantly, are there also other categories besides “soft” and “hard” targets when it comes to terrorism? For one thing, there are many more soft than hard(-ened) targets. Here are some typical hard (-ened) and soft targets recently exposed to terrorist attacks.

**Typical Hard Targets**

Typical hard targets include but are not limited to: individual top-level politicians, international summit meetings, government ministries, parliament, foreign embassies and diplomatic
residences, commercial passenger airplanes, nuclear facilities (power plants), military compounds, and prisons.

Hard targets are typically surrounded by physical deterrents such as barbed wire fences or high walls as well as vision barriers. There are vehicle barriers at the gates and armed guards with bullet proof vests supported by x-ray machines, metal detectors and sniffers to find hidden explosives, with CCTV cameras and infrared movement sensors to monitor the fenced or walled perimeter. Access points are few and checkpoints can be passed only after ID verification against a computer-linked database and following luggage/baggage and body screening.³

Typical Soft Targets

Typical soft targets include, but are not limited to: transportation systems (e.g. airport terminals, railway & bus stations, subway system, ferries) places of religious worship (e.g. churches, mosques, synagogues, temples), weddings, funerals, schools, hospitals, dormitories, market places, indoor shopping malls, museums, tourist destinations, hotels, restaurants, night clubs, theatres, cinemas, landmarks and iconic buildings with symbolic value, venues for special events, (e.g. sport stadiums, cultural arenas, concert halls), long queues of people at entrances gates to event sites, and pedestrian zones in urban areas.

Soft targets are undefended and/or under-protected open access locations with low or no security provided where civilians can be found in significant numbers.⁶ The Dutch intelligence service AIVD describes the distinction in these words: “… targets can be classified as “hard targets,” meaning well-protected targets, or as “soft targets,” meaning targets with little to no (possibility for) protection.”⁷

Types of Terrorist Targets

However, the sole distinction between just soft and hard targets is not all-encompassing, as it fails to recognize an important feature of terrorism. Terrorists are often engaged in a particular kind of psychological warfare, meaning that terrorist attacks are motivated by more than just the aim to cause physical harm. Above all, terrorism is a means to communicate, and the people victimised at soft and hard target sites serve mainly as message generators to reach, via mass- and social media, one or several other “targets” and objectives. Figure 1 visualises this notion of the use of terrorism as a communication tool.⁸

Figure 1. The Triangle of Terrorism
In a study published in the mid-1980s, the present author distinguished between four types of targets:\(^{10}\)

1. [Physical] targets of violence;
2. [Psychological] targets of terror;
3. Targets of (coercive) demands; and
4. Targets of attention

However, there are, in fact, more secondary and tertiary target audiences – targets of attention – to terrorist violence. These are ten terrorist audiences and/or conflict parties to be influenced:\(^{11}\)

1. adversary (-ies) – usually government(s);
2. society of the adversary (-ies);
3. direct victims and their relatives and friends;
4. others who have reason to fear that they might become next targets;
5. distrusted members and supporters of terrorist organizations (“traitors”);
6. other (rival) terrorist or political party organizations;
7. constituency terrorists claim to represent/act for;
8. potentially sympathetic sectors of domestic and foreign (diaspora) publics;
9. “neutral” distant publics which have not (yet) taken sides;
10. the media themselves, as message transmitters and amplifiers.

Looking only at the direct victims which are mostly found at soft target locations, misses the deeper meaning of terrorist victimisation. Yet, without direct physical victims, the terrorists’ violent message would not get a broad hearing and would therefore miss its main objective. The number of soft targets is almost endless, and if one soft target is hardened, terrorists can pick the next one of a seemingly unlimited choice of soft targets. In other words, displacement can make the hardening of specific targets a futile task as terrorists can move from a highly protected to a low security location. However, for most terrorists, the overarching aim is likely to bring their message across, “on air” and “online.” To put it differently, what really matters is whether their attack ends up being reported and discussed on television and on the internet. In our interconnected world, the physical location where a news-generating violent event takes place, has often become secondary. To illustrate this, the Christchurch shootings on a mosque and an Islamic centre in New Zealand on 15 March 2019 (where one hundred Muslims were injured or killed) was live-streamed on Facebook by the perpetrator Brenton Tarrant. Such events can have immediate reverberations on the other side of the globe, given the fact that social and mass media now serve as the nervous system of much of mankind.

However, newsworthiness also depends on the physical location of the attack, and, to a great extent, on specific types of victims since not all victimisations at soft or hardened target locations convey the same message with the same intensity. If we know what messages a specific group of terrorists wants to convey to its intended audiences, we already would possess an important indication of potential targets. This is to say that context matters very much and so does the type of terrorism we prioritise to respond to.

It is also helpful to be aware of the ten main types of terrorism:\(^{12}\)

1. single-issue terrorism;
2. lone wolf/actor terrorism;
3. vigilante terrorism;
4. separatist terrorism;
5. left-wing terrorism;
6. right-wing terrorism;
7. religious terrorism;
8. cyber terrorism;
9. CBRN terrorism; and
10. state (or regime) terrorism.

In the following, the focus is predominantly on an Islamist jihadist version of religious terrorism which has become the dominant type of transnational terrorism since 1979.

Protecting soft targets like people congregated in churches, synagogues and mosques or in outdoor spaces like at a Christmas market is a big challenge. There is a trade-off between keeping a society free and open, and keeping its citizens and visitors safe and secure. If the instruments of attack are everyday objects like a stolen truck driven at high speed into a crowd, there is not much that can be done downstream, in the minutes or seconds before it happens. Proactive measures like putting up physical security barriers – raising steel cylinders (bollards) hidden in the pavement in a public space to stop an approaching truck – takes more time than is usually available when such an attack seemingly comes out of the blue.

What then can be done realistically in terms of prevention and preparedness? To answer this question, we first have to look more closely at terrorist target selection.

**Factors Determining Terrorist Target Selection**

Typical for terrorists is to attack civilian and non-combatant targets; if terrorists would focus on military targets only, they would not be labelled terrorists but insurgents, guerrilla fighters, rebels, partisans, or perhaps resistance fighters. However, some terrorist groups attack, next to un- or ill-protected civilians, also police and military personnel, often when these are not on active duty. Such attacks are often also labelled terrorism, especially if they are conducted outside combat zones and in times of peace. While terrorist attacks are generally indiscriminate, they might be indiscriminate only within certain sub-groups of society.

Target selection is a function of several factors, including ideology, strategy, capabilities, and opportunities. The strongest of these tends to be ideology.\(^\text{13}\) There are a number of factors that help determine target selection by terrorists.\(^\text{14}\)

1. ideology;
2. strategy/tactic;
3. terrorist capabilities/resources;
4. opportunity;
5. newsworthiness;
6. expected counterterrorism security measures;
7. expected effects on supporters and sympathisers;
8. expected effects on other audiences and conflict parties (including rival groups);
9. internal decision-making processes within terrorist group preparing attack; and
10. post-incident getaway chances.

Ideology is the main determinant of target selection, even among non-religious terrorist groups. Luis de la Calle and Ignacio Sanchez-Cuenca looked at terrorist targeting in Western Europe over a forty-year period and analysed the distribution of 2,610 fatalities victimised by nationalist, extreme-left, vigilante, extreme-right, and neo-Nazi terrorists (see Table 1).

As can be expected, nationalist and leftist terrorists who claim to fight for the (or their) people prefer targeting representatives of the state, while vigilantes and those on the extreme right and neo-Nazis often tend to be more indiscriminate, target common people.

Turning now to religious terrorism and looking at data spanning the period 1994 to 2015, Petter Nesser found these patterns of Jihadist terrorism for Western Europe:

“It is noteworthy that as much as 70 percent of the plots involving single actors went undetected and reached the execution stage in the period surveyed, while
group-based plots were foiled in almost 80 percent of the cases.” (…) Over time, an increasing proportion of jihadi plots in Europe were discriminate and aimed at sub-national entities, communities and individuals rather than the public. (…)

Table 1. Target selection by ideology (1965-2005): Domestic terrorism in Western Europe - excluding jihadists

<table>
<thead>
<tr>
<th></th>
<th>Nationalist</th>
<th>Extreme-Left</th>
<th>Vigilante</th>
<th>Extreme-Right</th>
<th>Neo-Nazi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military</td>
<td>21.1</td>
<td>5.5</td>
<td>0.4</td>
<td>0.3</td>
<td>1.1</td>
</tr>
<tr>
<td>Police</td>
<td>33.2</td>
<td>47.8</td>
<td>1.2</td>
<td>7.8</td>
<td>2.2</td>
</tr>
<tr>
<td>Paramilitary</td>
<td>5.1</td>
<td>1.9</td>
<td>11.0</td>
<td>8.6</td>
<td>0.0</td>
</tr>
<tr>
<td>Politicians &amp;</td>
<td>3.2</td>
<td>13.3</td>
<td>0.2</td>
<td>0.8</td>
<td>0.4</td>
</tr>
<tr>
<td>public officials</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entrepreneurs</td>
<td>1.0</td>
<td>8.3</td>
<td>0.5</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Other civilians</td>
<td>36.5</td>
<td>23.0</td>
<td>86.7</td>
<td>82.5</td>
<td>96.3</td>
</tr>
</tbody>
</table>

In the period between 2001 and 2007, around 20 percent of plots were discriminate, whereas Al-Qaeda’s mass casualty modus operandi dominated the picture. In the subsequent period between 2008 and 2013, as many as 55 percent of all plots were targeted discriminate and random attacks were decreasing. The majority of discriminate plots were aimed at institutions, artists, and politicians, and perceived as anti-Islam.”

Indiscriminate attacks are not the same as attacks on soft targets. An attack on a synagogue, church, or mosque for example, is discriminate if we look at society as a whole – believers and non-believers – but also aimed at a soft target. According to a survey of terrorist attacks worldwide over the period 1968-2005, 72 percent (8,111 attacks) were aimed at soft targets, while 27 percent struck hard targets.

If we focus on religious terrorism of the Salafi-jihadist type, one study by the Norwegian researcher Cato Hemmingby, surveying 246 registered plots and initiated attacks in Europe between 1994 and the end of 2016, concluded:

“The main findings are that a soft target focus is dominant and increasing, while particularly well-protected targets are almost totally avoided. There is substantial mass casualty focus, but only few attacks lead to such results. Indiscriminate vs. discriminate targeting comes out evenly (…) Both lone actors and groups prefer soft targets …”

A more recent study by the Dutch Intelligence and Security Service (AIVD), surveying more than one hundred attacks in the period 2004-2018, concluded:

“Of the 112 attacks in the West in the past fifteen years, 76% can be considered succeeded, meaning that they were actually carried out and resulted in casualties and/or damage. The other 24% can be deemed failed; these attacks did not obtain the intended effect (damage or casualties), for example because explosives failed to detonate. In this regard too there has been a shift in the past fifteen years. During the first ten years of that period, half of all attacks succeeded, and half failed. In the past five years, however, the percentage of success has risen to 84%. So, not only have there been more attacks in the West
in the past five years (three-quarters of all attacks of the past fifteen years), but these attacks also succeeded more often.

(…) When considering the whole fifteen-year period, 30% of all attacks in the West occurred in freely accessible public locations where the victims were random passers-by or other people present in the area. In the majority of cases these were exterior locations like streets and squares, and in a small number of cases the location was a freely accessible building like a shopping centre or restaurant. Police officers were the target in 21% of attacks, while 15% of attacks targeted the military.\textsuperscript{19}

To summarize, the various surveys and studies referred to in this chapter provide us with two main takeaways. First, that soft targets are the main targets for both single actors and groups of terrorists and attacks on soft targets have been increasing. Second, most single actor plots went undetected while the detection rate for multi-actor attacks was considerably higher - but experts disagree on how many prevention efforts could be considered “successful” as criteria for success vary.

\textit{Prevention of Terrorist Attacks against Soft Targets: A Layered Approach}

After these more general observations, we can turn to what can be done to reduce harm to potential soft targets of terrorism. What is proposed here is a layered approach to the prevention of terrorist attacks – the idea being that more than a dozen preventive layers (PLM) should be created. While each of these layers might be insufficient to stop a terrorist attack, in combination these layers of defense can become a powerful instrument to prevent many if not most terrorist attacks - even in the case of soft targets.

Let us look at some of the possible prevention strategies and tactics. To begin with, one has to make a distinction between up-, mid-, and down-stream prevention. Terrorism prevention can be broken down into taking pro-active, precautionary measures at three moments in time. These phases of prevention of terrorism include:\textsuperscript{20}

- Upstream, primary (early) prevention: reducing the risk of the formation of a terrorist group or organization.
- Midstream, secondary (timely) prevention: reducing the risk of such a group or organization being able to prepare a terrorist campaign.
- Downstream, tertiary (late) prevention: reducing the risk of execution of individual terrorist operations by foiling and deterring these.

In other words, if terrorist group formation cannot be forestalled in an early phase by taking appropriate measures, the focus should be on preventing the preparation of terrorist campaigns in midstream and, if that also fails, prevention should seek to obstruct the occurrence of individual terrorist incidents.

Upstream prevention refers to structural measures that reduce the risk of terrorist attacks at the source and/or at an early stage, ideally even before terrorist group formation has taken place. Midstream prevention refers to situations halfway between root causes and events where a terrorist group is already formed. The goal here is to prevent a terrorist organisation from preparing a campaign of terrorist attacks. Downstream prevention refers to late prevention of specific and individual terrorist attacks.

In general, when one mentions prevention, one thinks more often of downstream and midstream prevention than of early, upstream prevention. While some of the upstream factors to prevent terrorism are beyond the control of a government (e.g. because the root causes lie
abroad) at least one root cause of terrorist attacks is not. Terrorist acts are often revenge acts against foreign armed conflict participation by governments abroad, or reactions to government human rights violations at home. This has been shown by the Institute for Economics and Peace (IEP) which uses empirical data on terrorist incidents from the University of Maryland covering a quarter of a century identified two major upstream root causes of non-governmental terrorism in its Global Terrorism Index report of 2016:

“Statistical analysis has identified two factors which are very closely associated with terrorist activity: political violence committed by the state and the existence of a broader armed conflict. The research finds that 92 per cent of all terrorist attacks over the past 25 years occurred in countries where state sponsored political violence was widespread, while 88 percent of attacks occurred in countries that were involved in violent conflicts. The link between these two factors and terrorism is so strong that less than 0.6 per cent of all terrorist attacks have occurred in countries without any ongoing conflict and any form of political terror [by government].”

In other words, not getting involved in armed conflicts and not violating human rights are two of the most important preventive measures that can be taken upstream. While the first measure – not getting involved in armed conflict – is not always a choice governments have since some governments are directly attacked even if they are not involved in foreign interventions, the second measure holding the moral high ground and adhering to human rights standards when fighting terrorism is a matter of choice and has been shown to reduce terrorism. Democratic countries with secure rule of law, good governance, and a high degree of social justice are less prone to terrorist attacks – at least from domestic and home-grown terrorists. Such policies – and the political culture that comes from a healthy relationship between government and civil society and between ethnic and other domestic majorities and minorities – tend to dissuade many activist local groups from escalating their militancy in the direction of terrorist attacks.

Related to such dissuasion is dissuasion’s stronger brother – deterrence. While deterrence is part of the instruments of prevention, its use in counter-terrorism is, however, limited. Deterrence depends on the fear of certain and severe punishment and retribution. However, one problem with deterrence of terrorists is that the perpetrators or groups responsible for terrorist attacks are hard to find; few have a known address where the perpetrators or their sponsors can be reached and punished before an attack. In the absence of the possibility of retaliation, deterrence is of limited utility. This is particularly true in the case of suicide bombers: if someone is not only risking his or her life in an attack but actively seeking death as a form of martyrdom in expectation of rewards in an imagined afterlife, the threat of being killed is absent and direct deterrence does not work. Sometimes it is, however, possible to threaten punishment for those who support terrorists. There are some indirect ways to deter attacks: if the families of terrorists are living at a known location, their houses can be bulldozed – a tactic familiar to Palestinians around Israel. However, that raises some important legal and ethical issues which, however, will not be discussed here.

If we look at the more familiar instruments available for terrorism prevention, most of them refer to downstream prevention. Here, time is short as the window between planning a terrorist attack and its execution is at best a few months and often only weeks or even less. Based on American data, Brent Smith, Kelly Damphousse, and Paxton Roberts noted in 2006 when analysing pre-attack planning and preparation of terrorist acts committed in the US:

“Planning and preparatory activities cannot be temporally separated. Meetings, preparation, training, and procurement of materials for terrorist incidents are
not sequenced independent of each other (...). The onset of preparatory behavior typically began about three to four months prior to the planned terrorist incident. Preparatory conduct may include criminal, as well as noncriminal activity. The most common preparatory behaviors included meetings, phone calls, the purchase of supplies and materials, and banking activities … Terrorist groups engaged in an average of 2.3 known behaviors per incident.27

A typical terrorist attack then is planned and prepared along the generic lines sketched by Charles Drake and Andrew Silke:28

1. Setting up a logistical network (safe houses, arms dumps, vehicles, ID, etc.). This is partially dependent upon how overt or covert the terrorists’ ordinary lives have to be.
2. Selection of potential targets – generally based on ideological and strategic considerations.
3. Information gathering on potential targets.
4. Reconnaissance of potential targets (find out the likely location and protection of the target at a specific time).
5. Planning of the operation.
6. Insertion of weapons into the area of operation.
7. Insertion of operators into the area of operation.
8. Execution of the operation.
9. Withdrawal of the operational team (not applicable if successful suicide attack).
10. Issue of communiqués if appropriate.

The short window of time when terrorist planning and preparations can be detected points to the importance of looking at, not only downstream signs of preparation, but also mid- and even upstream indicators. However, some methods of detection of upcoming terrorist activity apply to all three phases, the most important of which is intelligence gathering in all its forms, signal and human, self-generated, or received in exchanges with other intelligence- and security agencies. In the case of the 9/11 attacks on New York and Washington almost two dozen opportunities have been identified where US intelligence agencies could have intervened if they had interpreted the early warning signs correctly.

A Layered Approach to the Prevention of Terrorist Attacks, with a Focus on Soft Targets

In the following section, layers of preventive measures (LPM) that apply to mid- and downstream pre-incident detection and intervention tactics and measures in the case of terrorist attack planning and preparation are identified, accompanied by brief comments on each layer. The general assumption here is that we are facing an indiscriminate attack on an unprotected crowded place.29 The challenge is to pick up early warning signals and interpret these correctly. This is more difficult than simply connecting the proverbial dots. It is more in the nature of figuring out a puzzle with many missing pieces and, to make it worse, the pieces in front of the analyst most likely belong to more than one puzzle as several terrorist groups might be planning attacks on various targets. In such situations, linking the pieces to specific preparations becomes exceedingly difficult. The basic idea here is that while the target site is unprotected, there are intervention points at several mid- and downstream stages that can prevent the unprotected target site from being successfully hit. While these preventive measures are listed sequentially here, in reality their order might be different. A further assumption is that we are dealing with homegrown, domestic terrorism, rather than transnational terrorism, where planning and preparation occur largely abroad. In such border-crossing cases, prevention
becomes more difficult and depends very much on the close and time-sensitive international cooperation of intelligence and security agencies.

The 13 layers of preventive measures (LPMs) for mid- and down-stream soft target protection will be explained below.\(^{30}\)

**LPM 1: Engage in ongoing collection of traditional open-source information (print media, radio, TV, academic studies and NGO reports) by professional monitoring agencies.**

Explanation: Use Open-Source Information (OSI) to the fullest extent. While there is a certain mystique about secret intelligence, fact is that as much as 90 percent of all information intelligence agencies collect tends to come from open sources. Systematic data collection of traditional open-source information by academic institutions and think tanks can go a long way to make basic risk assessments when it comes to terrorism. The full exploitation of open-source information, when done in collaboration with academia, think tanks, and private sector stakeholders allows for basic monitoring of extremist groups and their activities and can help identify trends of targeting to discover patterns. Terrorist violence is often contagious; one new tactic, especially if successful, invites imitations by other groups or copycat crimes by mentally disturbed lone actors. Typical examples are increases in vehicle-based attacks and knife attacks. Sometimes terrorist spokesmen recommend certain easy-to-do attack types in video-messages on the internet and this tends to trigger a particular attack wave by gullible persons who identify with a terrorist cause without necessarily being part of a group. The thing to do, is to monitor terrorist communiques and other messages encouraging certain attack types. This is a form of mid- and downstream precaution which might not prevent a specific attack but it can also warn the public to look out for something that it would otherwise pay no attention to.

**LPM 2: Monitoring extremist online activities with potentially violent consequences (e.g., hate speech that can be a predictor of hate crimes, incl. terrorism) in social media and on the dark and deep nest.**

Explanation: The internet, to which now more than half of mankind has access, provides an abundance of additional information, and while many extremists try to hide behind encryption and in the deep and dark nets, they also have to reach out to potential recruits and appeal to their envisaged constituencies. Social media content can offer many cues. Monitoring hate speech is one measure that falls somewhere between midstream and downstream prevention. While most of those who engage in hate speech will not commit hate crimes themselves, incitement helps to create a political climate where hate crime, including terrorist crimes, are considered more legitimate among certain sectors of the public. Countering hate crimes is something that members of civil society can do as well, and sometimes better than government agencies. Its preventive effect is hard, if not impossible, to measure, but that should not be a reason for not monitoring and opposing hate speech. Monitoring hate speech is also necessary for late prevention. If, for instance, after a terrorist attack, people on the internet express support for a terrorist attack, they ought to be watched.

**LPM 3: Intelligence collection from surveillance and eavesdropping on known and suspected extremist individuals and groups, and their sponsors (e.g. by bugging their phones, computers, cars, and homes).**

Explanation: Surveillance and eavesdropping. Multiple methods of eavesdropping on terrorist communications exist and the main problem is not so much picking up such communications as decrypting, translating, and interpreting these in actionable time due to the huge volume of
internet traffic. Surveillance takes many forms beyond monitoring someone’s presence on the internet. Without technology (e.g. surveillance cameras which allow face recognition, car number registration, airline passenger identification, etc.) this cannot be done, as physical surveillance is personnel-intensive and costly, and beyond the means of all but very few governments. Surveillance can be done in various ways (e.g. bugging the homes, vehicles, phones and computers of suspects) if there are no legal restrictions. The thing to do is to monitor both former terrorists who have not deradicalized (e.g. those released from prison) and sympathisers of terrorist groups. Since this can apply to a large group of people, choices have to be made about the method and intensity of surveillance. This tactic would, however, not be successful against lone actors with homemade bombs. However, in many cases, such people might already have a criminal or a mental health history for which data exist and which might be worth looking into.

Given the multitude of soft targets, without guidance from collected intelligence, the defense of soft targets would be nearly hopeless. Intelligence, human and signal, open and classified, is the first line of defense. While many think the future is entirely unpredictable, fact is that many (but by no means all) events cast their shadows before them. Prognosis based on known precursor signals is possible to a certain extent. The detection, registration, and observation of more or less weak signals and indicators that point to the possibility and a growing probability of the occurrence of a harmful event requires monitoring in the form of systematic data-gathering. It also involves subsequent timely analysis and interpretation to produce risk assessments solid enough to forecast with a high degree of probability time and form of a terrorist attack. Then an early warning can be issued to those in the need to know and proactive rather than reactive counter-measures can be taken even when the exact location of the attack is not (yet) known.

**LPM 4:** Use of undercover agents for infiltration into violent groups and/or attracting informers from such groups (e.g. terrorists who are released from prison because they served their term and return to their group); use of sting operations where these are legal.

Explanation: Human intelligence. Due to the limitations of signal intelligence, human intelligence remains crucial. While infiltration of terrorist groups is difficult and dangerous (often a crime has to be committed first as proof of reliability when someone wants to join a group), winning informers from inside terrorist organisations or their support structures is a viable alternative. Unfortunately, the abundance of technical intelligence has in many agencies led to a neglect of cultivating human intelligence. Some intelligence services engage, in jurisdiction which allow to do so, in sting operations (entrapment) to attract militants seeking to obtain arms, ammunition and/or bomb-making equipment.

**LPM 5:** Exchange of finished (not raw) intelligence (signal and human), within and between government agencies, and with trusted intelligence- and security agencies abroad.

Explanation: Exchange of intelligence. Knowledge is power and information is knowledge. Its exchange between intelligence agencies within a country is often a problem and exchange between governments is an even bigger challenge due to, inter alia, source protection concerns. By exchanging only finished (not raw) intelligence, the problem of insufficient trust can be circumvented while it can result in the loss of actionable intelligence. Lack of sufficient reciprocity is often an obstacle to the exchange of sensitive intelligence but when it works between trusted partners it is of utmost relevance for the prevention of terrorist attacks. Time and again post-incident evaluations reveal that crucial information for prevention was “out
there” or even “on file” but was not widely shared or not shared in actionable time due to organisational barriers and for other reasons.

**LPM 6: Analyse terrorist propaganda and construct counter- and alternative narratives that are backed up by credible actions to prevent & counter (further) radicalization.**

Explanation: Terrorist propaganda often offers cues about the range of targets considered. Sometimes it has taken the form of open instructions in publications like *Inspire* (published by Al-Qaeda), or *Dabiq* and *Rumiyah* (published by ISIS). The study of public statements and captured documents from terrorist organisations offers important cues about likely targets.

**LPM 7: Encourage family members and friends of radicalising young men and women to confidentially report their concerns to a trusted organisation (not the police or intelligence services), while assuring them that this does not lead to the arrest of their family member or friend, but will bring them in contact with counsellors in youth mentoring or de-radicalization programs.**

Explanation: The terrorist incidents hardest to prevent are those of single actors or members of a single family (e.g. two brothers). Since few preparations can be carried out undetected by those closest to the perpetrators, reaching out to concerned family members and friends is important. However, these do not want to see their sons or daughters arrested and sent to jail. Therefore, assurances have to be given to them that what they report does not directly go to law enforcement, but will be handled discretely by psychological counsellors or deradicalization units.

**LPM 8: Monitor young people with a history of crime and/or mental health issues who appear inclined to join extremist groups and prepare special activity programs (e.g. sport and job training) for such youth at risk.**

Explanation: While in the past a sharp distinction has, and could be, made between common criminals and political offenders, that line has become blurred as almost half of all violent extremists tend to have – at least in Europe – a criminal record for violence, theft, robbery, or fraud. A smaller, but still sizable, number of such extremists – perhaps one-third – also have mental health issues. Some have both a criminal background and problems with their mental health. Such people need to be watched for signs of violent radicalization.

**LPM 9: Offer incentives to disillusioned members of terrorist organisations to leave their group and subsequently publicise, if they agree, their testimonies and help them start a new career.**

Explanation: To leave a terrorist network is difficult as traitors will be punished if not downright killed. This makes leaving hard and should, therefore, be assisted by middlemen. Few counter-narratives are as powerful as the testimonies of former insiders who can point out how big the gap between professed ideology and actual practice in a terrorist organisation really is.

**LPM 10: Offer rewards for information tip-offs from the general public that can help to prevent a terrorist attack and/or lead to the arrest of violent extremists and terrorists.**
Explanation: Since informing on terrorists (“snitching”) can be costly in terms of revenge acts, substantial sums of money need to be offered to those who cross the line and come forward with information that can help to stop a terrorist plot.

**LPM 11: Monitor and follow up specific ordinary crimes (such as theft of explosives) which might be perpetrated in connection with the preparation of a terrorist attack.**

Explanation: While some terrorist attack preparations are not unlawful in themselves, others are, and might come to the notice of law enforcement through different channels than those routinely dealing with countering terrorism. Things like theft of police uniforms or explosives, and purchases of ammunition ought, therefore, to be investigated. “Follow the precursor crime” should become as important as “follow the money” when it comes to preventing terrorist acts.

**LPM 12: Have rapid reaction protocols ready for dealing with credible attack warnings (e.g., on social media) received from the perpetrator or a spokesperson of the terrorist organisation.**

Explanation: Some terrorist groups (e.g., the Provisional IRA) provide[d] warnings of an imminent attack because they do not want mass casualties, or because they want that the public puts the blame on the government when it fails to evacuate an area in time. The time between a warning and an explosion is often very short. It is, therefore, important that protocols are ready to deal with credible attack warnings.

**LPM 13: Issue warnings via mass and social media to the general public when receiving credible new information about an impending terrorist attack and advise members of the public to be vigilant and look out for identified suspects and suspicious objects, opening a special phone hotline to report to responders.**

Explanation: Sometimes authorities are, without having received a specific warning from the perpetrator group, aware that an attack can happen any moment since they have multiple clues but lack information about where such an attack is about to take place. In such cases, the government can appeal to the public to report about the whereabouts of certain extremists on the loose and warn it about the likely danger. This can, in some cases, help to prevent an attack at the last moment or at least help to reduce the number of possible victims.

Are these 13 suggestions going beyond the state of the art? One way of ascertaining that is to compare these preventive layers with those developed by a working group of the Global Counter Terrorism Forum (GCTF) which includes 29 member states and the European Union. In 2017, the GCTF presented the Antalya Memorandum33 with 13 Good Practices (GP) on the Protection of Soft Targets in a Counterterrorism Context. These GCTF Good Practices (GP) for the Protection of Soft Targets34 include:

- **GP 1:** Be alert to the nature and history of the threat, monitor what terrorists are saying, and closely watch and learn from what they are doing.
- **GP 2:** Threat analysis should keep pace with the evolving nature of the threat and adversary, including local conditions and emerging technologies.
- **GP 3:** Conduct risk assessments.
- **GP 4:** Prioritize targets because not all targets are equal. Therefore, it is essential to identify and prioritize targets according to a risk assessment based on, and relevant to, local factors.
- **GP 5:** Align soft target and critical infrastructure protection efforts.
• GP 6: Include all stakeholders in establishing an effective national counterterrorism framework that clarify[s] responsibilities for soft target preparedness – prevention, protection, mitigation, response, recovery.
• GP 7: Enhance cooperation between and among all levels of government, between government and the private sector, and enhance the exchange of information and experiences between States.
• GP 8: Establish a trusted relationship between government and private sector security entities and encourage industry to play a proactive role in security efforts.
• GP 9: Citizens and private staff can contribute to security by reporting suspicious activity.
• GP10: Identify the right tool or measure for the right circumstance.
• GP11: Test assumptions and institute a lessons-learned program that incorporates analysis of previous attacks.
• GP 12: Train.
• GP13: Develop a communications plan (before an attack, during an attack after an attack).

While the 13 points of the Antalya Memorandum mainly emphasise organisational aspects of defensive prevention more generally, the 13 points suggested here rather focus on practical proactive prevention. However, while these two sets of recommendations are partly on different levels of abstraction, there are overlaps – Good Practices number 1, 7, 9, and 13 of the Antalya Memorandum largely correspond with Preventive Layer Measures number 6, 5, 9, and 10.

Conclusion

In its 2017 Antalya Memorandum, the working group of the Global Counter-Terrorism Forum concluded that:

“Protecting soft targets is complex. It is a perennial and practical struggle to balance security and access, and the target set is virtually unlimited. If casualties are the paramount terrorist metric for success, then every undefended group of people becomes a lucrative target.”

Given the reality that soft targets and crowded places are by definition unprotected or at least under-protected, preventive measures and interventions need to occur further upstream before a perpetrator can reach what the Antalya memorandum calls a “target set that is virtually unlimited.” In other words, prevention needs to occur before potential perpetrators have acquired arms and bombs and preferably also before they have joined an extremist group and before they have come to believe that an unprovoked terrorist attack on a random group of strangers is legitimate. In other words, rather than trying to harden an almost endless number of soft targets, multiple prevention layers that can act like filters should be applied before a terrorist attack is imminent in order to minimise the chances of an attack being planned and prepared at all. The main emphasis when it comes to soft target protection should be in the form of pre-incident plot detection, should be on preventing radicalization by, and recruitment into, terrorist organisations and, further upstream, on the prevention of terrorist group formation rather than on the costly hardening of multiple possible soft targets. Given the human cost of terrorist attacks and the costs of post-incident consequence management and recovery, such a shift of resources prevention in all its phases makes more sense.
Alex P. Schmid is a Research Fellow at the International Centre for Counter-Terrorism (ICCT) in the Hague, the Netherlands. He is Editor-in-Chief of Perspectives on Terrorism and former Co-Editor of Terrorism and Political Violence – both leading journals in the field of Terrorism Studies. Until 2009, Prof. em. Schmid held a chair in International Relations at the University of St. Andrews where he was also Director of the Centre for the Study of Terrorism and Political Violence (CSTPV). Previous positions include Officer-in-Charge of the Terrorism Prevention Branch of the UN Office on Drugs and Crime in Vienna and a chair in Conflict Resolution at the Erasmus University Rotterdam. Between 1978 and 2018 he also held various positions at Leiden University. Currently, he is Director of the Vienna-based Terrorism Research Initiative (TRI), a consortium of 16 institutes and more than 100 individual scholars seeking to enhance human security through collaborative research. Alex Schmid has more than 200 publication and reports in ten languages to his name, including the award-winning volume “Political Terrorism” (1984, 1988, 2006) and the “Routledge Handbook of Terrorism Research” (2011, 2013).
Appendix: Twelve Rules for Preventing and Countering Terrorism

By Alex P. Schmid

1. Try to address the underlying conflict issues exploited by the terrorists and work towards a peaceful solution while not making substantive concessions to the terrorists themselves.
2. Prevent radical individuals and groups from becoming terrorist extremists by confronting them with a mix of ‘carrot and stick’—tactics and search for effective counter-motivation measures.
3. Stimulate and encourage defection and conversion of free and imprisoned terrorists and find ways to reduce the support of aggrieved constituencies for terrorist organizations.
4. Deny terrorists access to arms, explosives, false identification documents, safe communication, safe travel and sanctuaries; disrupt and incapacitate their preparations and operations through infiltration, communication intercept, espionage and by limiting their criminal- and other fund-raising capabilities.
5. Reduce low-risk/high-gain opportunities for terrorists to strike by enhancing communications-, energy- and transportation-security, by hardening critical infrastructures and potential sites where mass casualties could occur and apply principles of situational crime prevention to the prevention of terrorism.
6. Keep in mind that terrorists seek publicity and exploit the media and the Internet to propagate their cause, glorify their attacks, win recruits, solicit donations, gather intelligence, disseminate terrorist know-how and communicate with their target audiences. Try to devise communication strategies to counter them in each of these areas.
7. Prepare for crisis— and consequence-management for both “regular” and “catastrophic” acts of terrorism in coordinated simulation exercises and educate first responders and the public on how to cope with terrorism.
8. Establish an Early Detection and Early Warning intelligence system against terrorism and other violent crimes on the interface between organized crime and political conflict.
9. Strengthen coordination of efforts against terrorism both within and between states; enhance international police and intelligence cooperation, and offer technical assistance to those countries lacking the know-how and means to upgrade their counter-terrorism instruments.
10. Show solidarity with, and offer support to, victims of terrorism at home and abroad.
11. Maintain the moral high-ground in the struggle with terrorists by defending and strengthening the rule of law, good governance, democracy and social justice and by matching your deeds with your words.
12. Last but not least: counter the ideologies, indoctrination and propaganda of secular and non-secular terrorists and try to get the upper hand in the war of ideas—the battle for the hearts and minds of those terrorists claim to speak and fight for.
Endnotes

3 Schmid, Alex P. (ed.). *The Routledge Handbook of Terrorism Research*. New York and London: Routledge, 2011, p. 604 and p. 620. Another author, Olivier Lewis, defines counter-terrorism in these terms: “… the countering (1) of deliberately indiscriminate violence, (2) of threats of indiscriminate violence, and (3) of political demands made via threats of indiscriminate violence. More simply, CT is an act that seeks to provide non-combatants with physical, psychological and political security” (…) “[Counter-terrorism] strategies can be divided in a number of different ways, but they all cover the same three goals: (1) strengthening social, psychological, and material resilience; (2) responding to attacks by giving medical aid to victims and prosecuting perpetrators; (3) preventing attacks (via coercion, persuasion, and cooption)…”; Lewis, Olivier, ‘Conceptualizing State Counterterrorism’; in: Scott N. Romaniuk et al (eds.). *The Palgrave Handbook of Global Counterterrorism Policy*. London: Palgrave, 2017, p. 20 & p. 27.
4 Terrorism is understood here as in this author’s revised *Academic Consensus Definition of 2011*: “Terrorism refers, on the one hand, to a doctrine about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence and, on the other hand, to a conspiratorial practice of calculated, demonstrative, direct violent action without legal or moral restraints, targeting mainly civilians and non-combatants, performed for its propagandistic and psychological effects on various audiences and conflict parties. Terrorism as a tactic is employed in three main contexts: (i) illegal state repression, (ii) propagandistic agitation by non-state actors in times of peace or outside zones of conflict and (iii) as an illicit tactic of irregular warfare employed by state- and non-state actors.” - Alex P. Schmid (ed.). *The Routledge Handbook of Terrorism Research*. London & New York: Routledge, 2011, p. 86. For the full academic consensus definition, see Available at: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/schmid-terrorism-definition/html.
7 Based on a great variety of sources, incl., for instance, Miller, Dennis H., Mary E., and Glover, Thomas J. *Pocket Partner*. Littleton. Colo.: Sequoia Publishing Inc., 2003, p. 240. - A Czech report noted that “There is no official definition for the term ‘soft targets. In …security circles, however, the term is used to denote places with high concentration of people and low
degree of security against assault, which creates an attractive target, especially for terrorists.
On the contrary, the so-called ‘hard targets’ are well secured and guarded premises....” - Kalvach, Zdenek et al., Basics of soft target protection – guidelines (2nd version). Prague: Soft Target Protection Institute, June 2016, pp. 6-7.
10 In this study from the mid-1980s, I explained in more detail that “… it is critical to define the ‘targets’ of terrorism. Terrorism involves targets both direct and indirect. Focusing attention on the wrong target, or on only one target, may cloud our understanding of the actual objectives of the terrorist act. First, there are targets of violence – random or symbolic victims usually sharing class or group characteristics (e.g. passengers for Israel at an airport) which form the basis for their selection. Through previous use of violence, or the credible threat of violence, other members of that group or class are put in a state of chronic fear. This group becomes the target of terror. The overall purpose of terrorism is either to immobilise the target of terror (in order to produce disorientation and/or compliance) or to influence the target of demands (e.g. governments) or targets of attention (e.g. public opinion).” - Alex P. Schmid, ‘Goals and Objectives of International Terrorism’; in: Michael Stohl and Robert Slater (eds.). Current Perspectives on Terrorism. New York: St. Martin’s Press, 1987, p. 48.
13 In a seminal dissertation on factors which influence the selection of physical targets by terrorist groups, Charles Drake concluded in 1996: “Several factors influence the selection of physical targets by non-state terrorist groups. These include the ideology of the terrorist group concerned, the strategy adopted by the group and its capabilities, its need to take account of external opinion - including that of supporters, the measures adopted to protect likely targets, and the security environment within which the terrorist group operates. (…) However, it can generally be said that ideology sets out the moral framework within which terrorists operate - and which determines whether terrorists judge it to be legitimate to attack a range of targets. After this, the determination of which targets it will actually be beneficial to attack depends upon the strategy which the group has adopted as a means of achieving its political objectives. The determination of their strategic objectives depends upon the effects which the terrorists hope their attacks will achieve. Thus, strategy further refines the range of targets initially delimited by the group’s ideology.” – Drake, C.J.M., The Factors which Influence the Selection of Physical Targets by Terrorist Groups. St. Andrews: University Ph.D. thesis, 1996. Available at: https://research-repository.st-andrews.ac.uk/handle/10023/2715 . - The decisive role of ideology also emerges from a statistical analysis done by Austin Wright: “Using novel data on Western European terrorism from 1965 to 2005 and a multinomial logistic extension of statistical backwards induction, I find that ideology is the only consistent predictor of target selection under strategic constraints.” - Austin I. Wright. Terrorism, Ideology and Target Selection. Princeton, N.J.: Princeton University, Working Paper, n. d.
14 Partly based on Silke, Andrew, ‘Understanding Terrorist Target Selection’. In: Richards, Anthony et al (eds.). Terrorism and the Olympics. London: Routledge, 2011, p.53 (Table 4.1. Key factors in terrorist target selection); Available at: https://www.academia.edu/6062416/Understanding_terrorist_target_selection .
16 Nesser, Petter. Islamist Terrorism in Europe. A History. London: Hurst, 2015, pp.59-60 & p.64. Nesser further noted that:” Another category of plots targeted military objects, in particular military personnel in public areas. A third category of plots targeted Jews. (…) A trend towards discriminate terrorism by jihadists in Europe is somewhat counterintuitive. Randomness is a hallmark of terrorism, given its aim of instilling fear in populations. Discriminate attacks are less suitable for frightening an overall population, but easier to justify politically and religiously than random ones.(…)Yet the threat against crowded public areas has largely remained constant (fifteen well-documented incidents before 2008 and nine in 2008-12). (…)The continued threat against public areas can only be interpreted as a sign that random mass casualty terrorism will not be fully abandoned by jihadis in Europe” (Idem, p.62).
22 The list of 12 rules for preventing and countering terrorism in the Appendix puts conflict resolution at the top of the list.
23 Cf. Parker, Tom. Avoiding the Terrorist Trap. Why Respect for Human Rights is the Key to Defeating Terrorism. London: World Scientific, 2019. See also Parker’s chapter 34 in this volume.
This scenario is based on the observation by the Dutch Intelligence and Security Service (AIVD) which concluded, looking at 112 attacks over the period 2004-2018: “The majority of attacks in the West in the past fifteen years (85%) was directed at easily approachable or accessible targets with little or no surrounding security measures. A relatively small number of attacks (8%) was directed against targets with some form of access control, for example entry tickets and bag checks. Of all attacks, 12% was directed against targets that were under physical protection by police officers or the military. Only 5% of all attacks in the West was directed against (very) well-protected targets, so called hard targets.” – Algemene Inlichtingen- en Veiligheidsdienst. Insights into targets. Fifteen years of jihadist attacks in the West. The Hague: AIVD/Ministry of the Interior, 2019, p. 20.

This list is based on multiple sources, including Bjørø, Tore, Strategies for Preventing Terrorism. New York: Palgrave Macmillan, 2013, pp. 55-70.

Bomb making at home is relatively easy since there are nearly 4,000 different chemicals which can be used to obtain an explosive reaction. However, the risk of unintended self-harm is high in inexperienced hands. – Kushner, Harvey W., Encyclopedia of Terrorism. Thousand Oaks: Sage Publications, 2003, p. 83.


Ibid.


Schmid, Alex P. “12 Rules for Preventing and Countering Terrorism,” Perspectives on Terrorism, Vol. VI, Issue 3, 2012; originally formulated at the end of his tenure (2005) as Officer-in-Charge of the Terrorism Prevention Branch of the UN Office on Drugs and Crime (UNODC, Vienna).
Bibliography


Li Piani, Tiziano, ‘Operative Guidelines for Protection of Places of Worship, a new approach
Torres-Soriano, Manuel Ricardo (2019), ‘How Do Terrorists Choose Their Targets for an Attack? The View from inside an Independent Cell’, Terrorism and Political Violence, Available at: https://doi.org/10.1080/09546553.2019.1613983
Web-based Resources


Counter-Extremism Project, Terror Targets, Available at: https://www.counterextremism.com/news-free-tags/terror-targets


GCTF, Initiative on the Protection of Soft Targets in a Counterterrorism Context. Available at: https://www.thegctf.org/What-we-do/Coordinating-Committee-Meetings/ArtMID/704/ArticleID/32

The Guardian, *From lizarding to lingering: how we really behave in public spaces*. Available at: https://www.theguardian.com/cities/gallery/2019/aug/01/lizarding-and-flex-allure-how-do-you-use-your-city-plaza-in-pictures-field-guide?fbclid=IwAR1ve4qaQ30bc4RLhEmCE8Qkjzv8cawBQJyggyPzn9yyF2TXPgFnghZi_dI

Jashari, Linda, *Soft Target Security: Environmental design and the deterrence of terrorist attacks on soft targets in aviation transportation*. Available at: https://www.hsaj.org/articles/14522


Lum Cynthia et al., *The effectiveness of Counter-Terrorism Strategies*. Available at: https://onlinelibrary.wiley.com/doi/10.4073/csr.2006.2

Moeler, Hans Mathias, *Why soft target terrorist attacks will remain a threat*. Available at: https://globalriskinsights.com/2016/07/soft-target-terrorist-attacks/


Securing soft targets and crowded places resources. Available at: https://www.cisa.gov/publication/securing-soft-targets-and-crowded-places-resources
Chapter 28

Prevention of Terrorist Attacks on Critical Infrastructure

Anneli Botha

Targeting critical infrastructure is an attempt to destabilize the social and economic functioning of the state and, therefore, will remain an extremely important concern for those tasked with prevention of terrorist attacks. The number of incidents grew substantially as a comparison of attacks between the periods 2000-2009 and 2010-2017 shows. While the threat of cyber-attacks against critical infrastructure is gaining momentum, the use of firearms and explosives still remains the preferred \textit{modus operandi}. As a result, the protection of critical infrastructure had been an important component of governments’ counterterrorism strategies in focusing on both traditional tactics and, more critically, on new technological advances such as the growing threat presented by Unmanned Aerial Vehicles (UAVs). Developing successful counter- and preventative measures starts with understanding the “enemy,” specifically the objectives, the political message, and capabilities of terrorist organizations. It also requires continuous risk, threat, and vulnerability assessments to plan and implement steps for anticipating and preventing infrastructure attacks.

Keywords: critical infrastructure protection, key resources, key assets, risk assessment, threat assessments, vulnerability assessments
Recognizing the multitude of targets of attacks against critical infrastructure – from individual hackers to hostile countries in cyberspace – one should not disregard physical attacks or a combination of cyber and physical attacks. These could be facilitated through a multitude of tactics from complex attacks involving the use of explosives (predominantly improvised explosive devices or IEDs) in combination with active shooters, hostage-takings, or the use of unmanned aerial vehicles (or UAVs). While the majority of the recent literature focuses predominantly on cyber rather than on “old school” physical attacks against critical infrastructure, this chapter will only focus on physical threats after first establishing what the concept “critical infrastructure” includes. This is followed by a discussion of the importance of threat, risk, and vulnerability assessments. A section on the manifestation of previous threats and incidents through utilizing the National Consortium for the Study of Terrorism and Responses to Terrorism’s (START) Global Terrorism Database (GTD) developed by the University of Maryland will introduce trends, weaknesses, and mitigating measures to be considered.

Working through earlier attacks, one is again reminded of the complex interconnected nature of infrastructure in that an attack on one service can have a direct impact on another. Energy, especially electricity, is the most critical sector, considering that none of the other sectors will be able to function without power. Although (so far) not caused by acts of terrorism, one only needs to consider the impact power outages have on the functioning of other sectors, e.g. the distribution of water, communication (especially internet connection), and fuel for power plants or reactors, whether delivered by road, rail, ship, or pipeline. Moreover, the vast and often long-distance distribution of critical infrastructure networks, for example the distance covered by oil pipelines, bridges, dams, and mobile phone towers further add strain to efforts to protect these facilities. Placing the entirety of critical infrastructure of a country on the table will create the impression of being impossible to protect, considering the resources and manpower required. However, an analysis of previous failed and successful attacks will come in handy while constantly conducting threat, risk, and vulnerability assessments on all levels – country, industry, and facility – while also keeping the unpredictability of terrorists in mind. As a result of this unpredictability of the attacker, any analysis needs to identify the “enemy” as far as possible, assessing their motivations, size, targets, and earlier modi operandi. The ultimate objective is to plan for the most probable contingencies, while not losing sight of less probable, but high impact, incidents.

This chapter will focus on the concept “critical infrastructure,” the manifestation of attacks directed against critical infrastructure – most notably transportation, utilities, and telecommunications – and how the state and private sector can respond to these ever-changing threats. While a country’s communication network, in particular cyber network, is part of critical infrastructure, cyber security is addressed in chapter 29 of this handbook.

**Terminology**

Determining what “critical infrastructure” should consist of, is almost as difficult as finding a broadly acceptable definition for “terrorism,” considering the implications of including and excluding some services and industries.

The US Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, identified 16 critical infrastructure sectors whose “assets, systems, and networks, whether physical or virtual, are considered so vital to the country that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”¹ These include:

1. Energy (e.g., oil, gas, wind turbines, solar farms) that is needed in the production of electricity, its storage and distribution. Nuclear reactors and waste management.
2. Transportation to include all possible forms of transportation from road, rail, air (airplanes and airports, as well as air traffic), sea, and inland waterway transport. Considering that these networks extend beyond the country’s borders this section will also make provision for border security and surveillance.

3. Information systems that include, for example, the internet (the system and protecting the physical network as well as mobile and fixed telecommunication and satellites, also needed for navigation).

4. Communication sector that includes broadcasting through television and radio.

5. Water and wastewater systems (sewerage farms) that include dams, and monitoring and maintaining the provision of purified water.

6. Food and agriculture aimed at the production and delivery of food suitable for human consumption.

7. Chemical industries that require caution and management in the production and storage of dangerous substances.


9. Emergency services.

10. Financial services with reference to banking and payment services.


12. Commercial facilities that draw large crowds of people for shopping, business, entertainment, or lodging.

13. National monuments that are important in representing a country’s national identity as well as religious institutions with references to churches, mosques, and synagogues. Symbolism in attacking these facilities and the emotional reaction following an attack make it a favorable target in hate crimes (targeting only the facility) to severe incidents of hate crimes and acts of terrorism.


15. Defense sector that enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems and components or parts.

According to John Moteff, Claudia Copeland, and John Fischer, critical infrastructures also include national monuments “where an attack might cause a large loss of life or adversely affect the nation’s morale.” Attacks against critical infrastructure and monuments are also clearly incorporated in the African Union’s definition of a “terrorist act” as presented in Article 1 (3) of the 1999 Organization of African Unity (OAU) Convention on the Prevention and Combating of Terrorism:

(a) “any act which is a violation of the criminal laws of a State Party and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to, any person, any number or group of persons or causes or may cause damage to public or private property, natural resources, environmental or cultural heritage and is calculated or intended to:

(i) intimidate, put fear into, force, coerce or induce a government, body, institution, the general public or a segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular standpoint, or act according to certain principles; or

(ii) disrupt any public service, the delivery of an essential service to the public, or to create a public emergency; or

(iii) create general insurrection in a State.”

While this definition also captures some of the main objectives of terrorism, the possibility exists that what is regarded today as critical by governments, might not be regarded as such by tomorrow’s terrorists. The focus might shift from merely physical attacks towards more attacks on critical infrastructure in cyberspace, which would require different countermeasures While
terrorist organizations, such as the Islamic State in Iraq and Syria (ISIS) and Al-Qaeda, became more active in cyberspace in recent years, and might soon be able to cause substantial damage in new ways, the predominant terrorist inclination still is to rely on physical tangible tactics, at least till cyber-attacks become physically visible. Considering the technical skills required to launch major attacks in cyberspace, it is likely that, in the near future, most terrorists will make use of explosives, firearms, and knives to carry out their next attack.

**Determine the Nature of the Threat**

The debate around what should be included when referring to “critical infrastructure” is often influenced by cost implications (i.e. costs of resorting an infrastructure object) if and when a building, network, or service is categorized as such. The level of security associated with the protection of above will be influenced by the level of threat (likelihood of becoming a target) and the classification of countermeasures put in place to address potential threats. The former will require risk, threat, and vulnerability assessments.

According to John Ellis, risk assessment “is a concept developed in many settings to analyze the possibilities or probabilities of future events and circumstances, and then forecast the impact this would have on the organization conducting the assessment and on its goals.” Risk assessments, however, often only provide a snapshot of the vulnerabilities in what is an ever-changing environment. Good forecasts should be based on the history of threats and incidents, given that there usually is a high probability that history will repeat itself at some point in time. Forecasting will also require a careful consideration of existing circumstances and indicators that will determine the probability of certain outcomes.

Ideally, risk assessments should be regularly undertaken to deal with changing trends and capabilities of security forces. This way both current and future threats can be monitored and addressed accordingly.

Terrorism-related risk analysis has been defined by Hunsicker as:

> “a survey to ascertain how high the probability is of one of these dangers occurring, how well the organization can respond should the threat become a reality, and how well the organization can carry on once that reality materializes. Inherent in the analysis is the identification of the vulnerabilities and threats that go along with the risk. In the course of the analysis, one of the things to be determined is the extent of the organization’s exposure, which could materially contribute to loss or damage in the event of a terrorist attack.”

Considering that not every sector or facility can receive the same level of protection, the level of risk needs to be calculated. The first step is to determine the value of each asset (e.g., human beings, facilities, services, processes and programs). The second step is to determine what the impact would be if the asset is damaged or destroyed. Based on such calculations the standard classification system will express risk on a five-point scale as: i) very low, ii) low, iii) moderate, iv) high, or v) extremely high. According to Moteff and Parfomak, the value of an asset can also be expressed “in monetary terms in what it will cost to replace an asset from the cost to build the asset, the cost to obtain a temporary replacement for the asset, the permanent replacement cost for the asset, costs associated with the loss of revenue, an assigned cost for the loss of human life or degradation of environmental resources, costs to public/stakeholder relations, legal and liability costs, and the costs of increased regulatory oversight.”

The US Department of Defense focuses on the following four critical components to evaluate and prioritize the protection of its assets:
1. Criticality: how essential is the asset?
2. Vulnerability: how susceptible is the asset to surveillance or attack?
3. The ability to reconstitute: how hard will it be to recover from inflicted damage?
4. Threat: how probable is an attack on this asset?

It is important to factor probabilities into the broader threat and vulnerability assessments.

Threat assessments are originated from, and are primarily used by, security forces when they have to decide on the best strategy to address (e.g., a specific threat to national security). In essence, a threat analysis is based on the need to identify, prioritize, and monitor the most hazardous threats to human safety and security. In conducting a threat assessment on terrorist activities within a specific region, certain information is required to build a profile that will be used to assess the level of threat and the most appropriate counteraction. This information needs to include, for example, the existence of groups that currently or previously resorted to violence and other acts of terrorism in a specific country. This will have a direct bearing on the risk portion and on the validity of the vulnerability analysis. In other words, an important relationship exists between threat and vulnerability that requires constant re-evaluation.

Although an existing threat profile might form the foundation of this assessment, other factors also need to be taken into consideration. For example, with reference to critical infrastructure, the profile of the facility or establishment, and the type of shops and events hosted in shopping centers (e.g., live events might include celebrities or prominent officials that most often receive media coverage), need to be taken into consideration. Vulnerability assessments determine whether a specific country or institution might be vulnerable to terrorism or other risks. Therefore, risk and threat assessments serve as a foundation for vulnerability assessments.

Before embarking on a threat analysis, the first question to be asked, is: “For what purpose?” The answer will determine the model and the specific categories used to conduct the assessment. It is again necessary to stress the importance of realizing that although risk, vulnerability, and threat assessments may fall under predetermined categories, decisions will be determined by the aim and objective of the assessment. Within risk assessment and vulnerability analysis the focus is to determine what you are facing and how it will affect you. For government security forces the aim will be to prevent or deter the risk (proactive), defend (pro- and re-active), and respond or use the best strategy to manage the actual risk when it occurs (re-active).

Essentially, the vulnerability analysis focuses on the identification of all factors, including safety and security hazards that leave people or critical infrastructures vulnerable to attacks. As a consequence, the aim of a vulnerability assessment is broader than a risk or threat analysis. Accordingly, the aim is not only to identify potential threats, but also to understand their likelihood of occurring. The goal therefore is twofold.

Firstly, the aim is to identify threats - in this case terrorism - based on feasibility and indicators of potential exploitation. For example, the existing presence of a known terrorist organization operating or intelligence on the presence of individuals suspected to be involved in decentralized networks. Al-Shabaab in Eastern Africa is an example of the former that were previously implicated in numerous attacks on above classification of critical infrastructure, namely prominent shopping centers (for example the Westgate shopping mall attack on 21 September 2013 and the DusitD2 complex attack on 16 January 2019) and Kenya’s mobile communication network in the Northeast region close to the border with Somalia. This type of threat manifests in countries the closest to conflict areas, for example Somalia where attacks are being planned and executed from both Somalia (origin) and/or Kenya (extension).

Another factor that will increase vulnerability is the manifestation and extent of domestic marginalization on the basis of religion and/or ethnicity (often associated with a decreasing national identity) that the organization can exploit. These threats are further categorized by the
likelihood that vulnerabilities will be exploited. In the case of Kenya, the presence of its defense force in Somalia as part of the African Union Mission to Somalia (AMISOM) increased the likelihood of attacks in Kenya. This category is directly linked to the motivation or what attackers hope to achieve. For example, in the case of Kenya, the aim was to intimidate the country through attacks on its population so as to pressure Kenyan armed forces to withdraw from Somalia. However, attacks can also facilitate the future operation of the organization. For example, destroying telephone masts (sabotage) prevents the public from reporting the local presence of al-Shabaab fighters to authorities. Through isolating these often-remote areas, the organization enhances its presence in the country and weakens the Kenyan state by showing the immediate community - but also the broader country - that government is unable to maintain control over its territory and cannot protect its citizens from external threats or from threats emerging from refugee camps and illegal immigrants. Although the presence of illegal immigrants is not an immediate threat per se, limitations associated with the legal status can increase future vulnerability as these individuals will be exploited, while not enjoying the same benefits as citizens. Most critical for assessments is the identification of infrastructure lacking effective security measures.

The second aim of a vulnerability assessment is to provide an informed assessment based on detecting, monitoring and predicting potential threats. As a multivariate analysis, the aim of a vulnerability assessment would be to predict future trends on the basis of current and historical information; and describe and understand the underlying relationship within a country that could ultimately determine the vulnerability of a country to instability and terrorism.

Attraction of Launching Attacks against Critical Infrastructure

Determining the potential threat, risk, and vulnerability is the first step in establishing the value and need to protect a particular asset, from the perspective of those launching an attack as it is important to determine the value of attacking that particular target. In this regard the motive behind spending time (in planning the attack), resources (what is needed to execute the attack) and the risk (of being killed or captured) will be taken into consideration in determining the risk and what is needed to protect and counter a possible attack. It is, therefore, important to recognize the different values that will be attached to an asset by terrorists and criminals, because this difference will influence the type of countermeasures needed to protect that particular asset.

Similar to other criminal activities, the motive (intent) behind the attack is an important factor for understanding, countering, and preventing future attacks as it sheds light onto the potential modus operandi and the value of each target. These can include:

- Attacks directed at the infrastructure aimed at physically destroying the building, airplane, airport, refinery, mobile phone mast etc., to disrupt the service where the aim is not to cause mass casualties.
- Attacks against personnel employed at facilities: These specifically directed attacks (discriminate) through killing, kidnapping etc., persons for their symbolic value, but also to attain access to the facility.
- Attacks against passengers or the broader public, making use of all forms of transportation that is generally indiscriminate (being at the wrong place at the wrong time) and intended to cause mass casualties.
- Intimidation directed at the intended target, but also broader audiences that might find themselves in a similar situation in the future.\textsuperscript{15}

From the perspective of terrorists, there are a number of factors that will influence their decision-making process:\textsuperscript{16}
Symbolism: Symbolism can be defined as something that stands for or suggests something else; especially a visible sign of something invisible.” Keeping in mind that attacking a specific target is a form of communication, deciding on a specific target is, among other motivations, also driven by symbolism: the greater the symbolic value of the target, the more publicity the attack brings to the terrorists and the more fear it generates. Symbolism can also rationalize the decision to focus on a particular target in representing what the attackers are against. For example, in the minds of those who planned the 9/11 attacks, the World Trade Centre symbolized capitalism and the financial strength of the US, and the Pentagon its military power. The symbolism of these targets was clear and the attacks were categorized as acts of symbolic terror within the framework of political communication. Attacking the Independence Day celebrations in Nigeria, the Movement for the Emancipation of the Niger Delta (MEND) not only ventured outside its normal area of operation (the Niger Delta) and its traditional target selection (oil companies), but it also attacked the Nigerian state, its unity and its accomplishments when celebrating fifty years of independence.

Vulnerability: When planning an attack, those involved in this process will consider how protected and secure the target is. Although it might be easier to attack a soft target in comparison to a hardened target, the message in successfully attacking a target that is regarded as “secured,” associated with the intimidation value (benefit), might surpass the risk. The differentiation between “soft” and “hard” targets, therefore, predominantly rests upon the level of access control and steps being taken to prevent incidents (security).

Risk: What is the risk of detection and being captured? In other words, is the risk worth the effort?

Feasibility: Is the target accessible? Will the intended level of destruction be achieved? How easy and expensive will it be to rebuild and recover?

Impact: Will attacking the target bring about the required result (i.e., the anticipated impact on its intended victims and the audiences watching the attacks)?

Reflection on the organization: How will the organization be perceived after the execution of the attack, considering that “overkill” (resulting in more than the expected casualties) will reflect negatively on the organization?

The last element is particularly important when the terrorist organization relies on the support of a segment within the public. For example, following the attack in Mogadishu, Somalia on 14 October 2017 in which 587 people were killed and 316 people were seriously injured, no organization claimed responsibility. According to all indications al-Shabaab (suspected to be responsible) did not intend to cause so many casualties as the device most probably was detonated prematurely by its driver when it was stopped by security officials while stuck in a traffic jam. A nearby fuel tanker ignited and caused a secondary explosion that increased the number of casualties. This same element will be less relevant when the organization or individuals involved in planning an attack is detached from the country and the public targeted. For example, the 9/11 attackers had no attachment to the US, but were external actors launching attacks against the US with the intention to cause as many casualties and as much destruction as possible. The same consideration is also relevant to other attacks in Europe. For example the 2004 Madrid train bombings when ten IEDs detonated on four commuter trains, resulting in the death of 191 people and nearly 2,000 injured, and the 2005 attacks on the London Underground and a bus at Tavistock Square in which 52 people were killed and approximately 700 injured. Although these attacks were executed by nationals, some with links to immigrant communities, those executing the attacks associated themselves with an external cause (withdrawing support from the US alliance and involvement in
especially Iraq). It is equally important to note that all of these attacks were directed at a critical infrastructure - the transportation sector of Spain and the UK.

Understanding the organization, its objectives, and its ideology will ultimately shed light onto its target selection process and its modus operandi. Furthermore, from the perspective of the state, responsible for protecting an array of potential targets, it is critical to prioritize vulnerabilities and risks within the framework of its broader terrorism threat assessment, an assessment that need to be constantly updated.

**Type of Threats**

Although the following section will reflect on previous attacks, this is not at all an indication to those involved in planning for critical infrastructure protection to exclude what may happen in the future. Those tasked with prevention should put themselves in the shoes of potential attackers (think like a “terrorist” also referred to as “red teaming”) and, from the adversary’s perspective, recognize weaknesses. Terrorists’ success lies in their ability to change or adapt old and new tactics to their operations. In preparing for a potential act of terrorism, security forces often prepare only for the known instead of thinking “outside the box” and also prepare for the unfamiliar.

The modus operandi and target selection will be determined by the objective of the attack and the availability of appropriate means. For instance, ISIS had a dedicated article in its magazine *Rumiyah* on how to use fire as a modus operandi: “Ideal target locations for arson include houses and apartment buildings, forest areas adjacent to residential areas, factories that produce cars, furniture, clothing, flammable substances, etc., gas stations, hospitals, bars, dance clubs, night clubs, banks, car showrooms, schools, universities, as well as churches, Rafidi temples, and so forth. The options are vast, leaving no excuse for delay.”

In addition to arson, terrorist weapons and methods include:

- **Explosives:** Particularly Improvised Explosive Devices (IEDs) come in many forms and use various delivery methods. Bombing is, historically, the most common terrorist tactic for two main reasons: Relative low risk to the organization when compared to the benefits and the physical (destruction) and psychological impact on the target, especially when the attacker is willing to commit suicide. The UN through the International Convention for the Suppression of Terrorist Bombing in 1997 criminalized bombings, “including the delivery, placing, discharging or detonating an explosive or other lethal device in, into or against a place of public use, a state or government facility, a public transportation system or an infrastructure facility with the intent to cause death or serious bodily injury or extensive destruction to property.”

- **Firearms:** terrorists use various types of firearms for attacks that are discriminate (for example in the case of assassinations) or indiscriminate (when the attacker indiscriminately shoots into a group of people).

- **Knives** (including for decapitation): the propaganda and intimidation value of knitting has been refined by Al-Qaeda in Iraq under Abu Musab al-Zarqawi and, more recently, by ISIS. The latter in its magazine *Rumiyah* dedicated a feature on the use of knives, including for decapitation, by giving detailed instruction of the type of knives that should be used for various forms of killing.

- **Kidnapping and hostage taking:** this tactic is used to achieve a number of objectives, ranging from extorting ransom (money to fund the organization and other activities – not for personal financial gain) to propaganda purposes (particularly when hostages are being executed and the video material is distributed on the Internet). ISIS in the ninth issue of *Rumiyah*: “The scenario for such an attack is that one assaults a busy,
public, and enclosed location and rounds up the kuffar who are present. Having gained control over the victims, one should then proceed to slaughter as many of them as one possibly can before the initial police response …”

Under the heading “Ideal target locations” the article continues “… generally any busy enclosed area, as such an environment allows for one to take control of the situation by rounding up the kuffar present inside and allows one to massacre them while using the building as a natural defense against any responding force attempting to enter and bring the operation to a quick halt.”

- Hijacking: this signifies the hijacking of airplanes, vessels, and other forms of public transport. The propaganda value (and media coverage) of attacking people in transit was realized early in the development of transnational terrorism. As a result, the first international conventions dealing with terrorism concentrated on the hijacking of airplanes and the security of aviation on the ground.

With the above arsenal at their disposal, numerous terrorist attacks were directed at utilities (electricity, gas, and oil) and transportation systems (see Figure 1 for a breakdown of attacks between 2000 and 2017), with firearms as the preferred weapon of choice (see Figure 2).

**Figure 1. Attacks against Critical Infrastructure 2000 until 2017**
Airports and Airplanes

Although attacks on aircraft in flight is not new, the format has slightly changed over the years, as has been reflected in the UN conventions and protocols against the different forms of terrorism. The 1961 Tokyo Convention, focusing on offences committed on aircraft, and the 1970 The Hague convention, addressing plane hijackings, were followed by the 1971 Montreal Convention that criminalized the placement of explosives on board and sabotage, interfering with the navigation systems of the aircraft and damage to the plane that will endanger the safety of an aircraft in flight. Following 9/11, the UN responded by introducing the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, signed at Beijing on 10 September 2010. The 2010 Protocol Supplementary to The Convention For The Suppression of Unlawful Seizure of Aircraft (1970 The Hague Convention) criminalized “violence against any person on board an aircraft in flight, endangering the safety of an aircraft, destroy or damage aircraft in service, destroy or damage air navigation system or interfering with its operation, use an aircraft in service for the purpose of causing death, injury or damage to property, transporting explosives or any biological, chemical and nuclear weapon (BCN) or radioactive material for the purpose of causing death, injury or damage, and threatening to commit such acts.”

In the period 2000-2017 the number of hijackings decreased substantially from 27 incidents during the period 2000-2009 (including 9/11) to only five incidents between 2010 and 2017.

The threat of explosives onboard airplanes was real and, despite the introduction of reactive measures following the uncovering of plots, bore witness to the negative application of people’s imagination. On 22 December 2001, Richard Reid (“the shoe bomber”) attempted to ignite explosives hidden in the heel of his shoes on a flight from Paris to Miami. In another failed attack, on 25 December 2009, Umar Farouk Abdulmutallab (“the underwear bomber”) attempted to detonate explosives hidden in his pants on a flight from Amsterdam to Detroit. In potentially the most devastating airline plot, in 2006 security forces arrested 24 suspects in London, who were associated with the liquid bomb plot intended to target seven transatlantic
planes in flight. Key components of the homemade explosives were acetone peroxide (TATP) and hexamethylene triperoxide diamine (HMTD) carried in 500ml soft drink bottles. As a result, 2006 regulations imposed a 100ml limit for liquids, aerosols, and gels to be carried inside a plane. Although this restriction is still in effect, the argument against these measures is that if a few passengers each carrying 5 x 100ml containers under this rule will not raise suspicion. Similarly, countering the underwear bomber and shoe bomber (although certain airline security companies require the x-ray screening of shoes) the central question is: do those operating x-ray machines know what to look for? In all this author’s travels across Africa, none of the security personnel could tell her why they had to screen shoes or why it is not allowed to carry more than 100ml in a container. Considering that airport security and the person manning the x-ray machine is the last line of defense, much more needs to be done to move from window-dressing security to a constructive barrier.

Following the successful detonation of explosives hidden in a laptop on a flight in Somalia on 2 February 2016, the US government restricted the ability to travel to the US with electronic devices from a number of countries, including: Jordan, Egypt, Turkey, Saudi Arabia, Morocco, Qatar, Kuwait, and the United Arab Emirates. Similar to this measure, the UK banned tablets, laptops, games consoles, and other devices larger than a mobile phone on inbound flights from Egypt, Jordan, Lebanon, Saudi Arabia, Tunisia, and Turkey. The main objective of detonating small charges in mid-flight has to do with the consequences of detonating even a very small charge in a pressurized cabin when reaching cruising altitude of approximately 35,000 feet (about 20 minutes after takeoff). Approximately 340 grams (12 ounces) of explosives detonated at an altitude of 31,000 feet brought down Pan Am 103 over Lockerbie, Scotland, in 1988.

Although explosives traditionally raised the most concern, airport security also placed a ban on knives, nail clippers, scissors, and even tweezers after 9/11. During the 9/11 hijackings the perpetrators used box cutters to gain access to the cockpit. However, despite these measures, the reality is that where there is a will there will nearly always be a way. Therefore, instead of boarding with a potential weapon, terrorists might use what is available on the plane. For example, buying a glass bottle on duty free and breaking it can produce an instant weapon.
The most effective way of managing this type of attacks will most probably be to enhance sky marshal programs – a strategy predominately introduced in the aftermath of 9/11.

**Surface-To-Air Missiles or Man Portable Air Defense Systems (SAM/MANPADS)**

The Surface-To-Air Missiles (SAM) or Man Portable Air Defense Systems (MANPADS) presents probably one of the most severe challenges to airplanes today, having an engagement rate up to 25,000 feet. Especially (though not exclusively) after takeoff and before landing (at an engagement range of approximately four miles) airplanes are particularly vulnerable. Although these weapon systems are particularly used in conflict zones and even directed at planes transporting humanitarian aid (most notably in Afghanistan and Somalia), the use of SAMs against commercial airliners has increased in recent years.41

For example, on 20 July 2019, British Airways and Lufthansa suspended flights to Cairo and North Sinai, due to security concerns. While Lufthansa resumed flights on 21 July, British Airways kept the ban for seven days.42 Although the exact nature of the threat was not made publicly known, unconfirmed intelligence sources indicated that violent extremist groups in Egypt planned to down a commercial airplane with a MANPAD. Five years prior, in January 2014, Ansar Bait al-Maqdis (which later became the Sinai branch of ISIS in, had used a MANPAD it obtained from Libya to shoot down an Egyptian military helicopter in the Sinai Peninsula.43 The following year, on 31 October 2015, the same organization had claimed responsibility for the attack on Metrojet Flight 9268, an Airbus A321-237, after it had taken off from Sharm El Sheikh International Airport. In this attack a small explosive device had detonated in mid-air at 31,000 feet.44

Considering the number of planes that were targeted by SAMs in recent years, other airlines should consider following Israeli commercial airline El Al’s example by rolling out anti-ballistic technology. This step came in response to attacks on 28 November 2002 in Mombasa, Kenya when two Strela 2 missiles were fired during take-off at an Israeli Arkia airline plane, - a Boeing 757 carrying 261 passengers - but missed.45 In February 2014 Israel’s Ministry of Defense (Misrad HaBitahon) announced that it successfully tested a “Commercial Multi-Spectral Infrared Countermeasures (C-MUSIC) system. According to Janes, a commercial intelligence firm, this new system consists of a pod under the fuselage that houses an infrared missile-tracking camera, an “infrared (IR), ultra-violet (UV), or radar missile-approach warning (MAWS) sensor to detect a missile launch in the very early stages of an attack” and a laser system meant to jam the incoming missile’s “seeker” and “cause [the missile] to be diverted away from the aircraft.”46 The system, however, only protects against shoulder-launched heat-seeking missiles and not against radar-based anti-aircraft missile systems, as in the case of the Russian SA-11 that downed Malaysian Airlines MH17 while the plane was at cruising altitude over the Ukraine, killing nearly 300 people.47 While the Israeli system is costly, more airlines ought to consider similar defense systems, especially when operating in high-risk environments or if the country itself has a high-risk profile.

**Unmanned Aerial Vehicles (UAVs - Drones)**

Although the use of UAVs by security forces are well documented, the use of commercial drones by terrorists is increasing and raising is concerns. Early on, ISIS started to use UAVs to collect intelligence before executing attacks, but the group soon learned to use it also as a mini-bomber. On 24 January 2017, the ISIS media office in Iraq’s Ninawa province released a video with the title “The Knights of the Dawawin.”48 It highlighted a new ISIS drone capability: dropping small bomb-like munitions on its enemies from the air. The capability displayed was not a once-off achievement as in scene after scene the video shows the group dropping small bombs from remotely controlled drones with some degree of accuracy. This
included ISIS being able to successfully drop munitions onto crowds, and to hit stationary vehicles and tanks while another drone lingered above and filmed the attacks. A few days later, on 30 January 2017, ISIS’ Wilayat al-Furat media office released a video entitled “Roar of the Lions” in which ISIS featured its aerial operation in the Anbar Province of Iraq. At the end of the video, the group showed a video clip of the drone being used to deliver an IED in Anbar. A year later, on 26 July 2018, Houthi rebels from Yemen claimed they had launched a drone attack on the Abu Dhabi airport. Although the United Arab Emirates (UAE) deny that the incident occurred, information available in the public domain claims evidence that the Houthis’ Sammad-3 drone launched three attacks on the airport.

Nine days after this incident, on 4 August 2018, two DJI M600 drones (manufactured in China), each carrying one kilogram of C-4 explosives, were used in a failed assassination attempt against Venezuelan President Nicolás Maduro, when one or both drones detonated explosives above the audience at a nationally televised military event. Although several people were injured, the president and his wife who was standing next to him onstage remained unharmed.

This was followed in December 2018 by an incident at London’s Gatwick Airport when a number of drone sightings brought the airport’s entire air traffic to a standstill. It later became known that this was not the first drone experience at Gatwick. In July of the same year there had been a near-miss between an unmanned aircraft and a passenger plane. According to the British Airline Pilots Association, the number of incidents involving drones and other aircraft has grown dramatically, from none in 2013 to 93 in 2017, to 117 incidents between January and November 2018.

Weaponized drones offer tactical advantages that only wait to be harnessed by terrorists (and criminals alike):

1. Versatility: with fixed-wing drones being able to fly much further from their controller than quad-copter versions, while the latter are able to hover and stay in one place.
2. Stealth: as most drones can fly lower than current technology (for example, radar) is capable to detect.
3. Thinking bomb: payload and utilization enables drones to be used in almost every phase of a terrorist operation. Being equipped with a camera, drones can be used to conduct surveillance on a potential target, whereas a camera with video link to the controller can be used in the execution of an attack to ensure accuracy that translates into executing the strike at the right moment. This allows the attacker to utilize the benefits of a suicide bomber as a ‘thinking bomb’ while enabling the controller to leave the scene unscathed to strike – unlike suicide bombers - at another target in the future.
4. Lethality: considering that even a small quantity of explosives can bring down a civilian aircraft in flight, commercial airliners are vulnerable to drone attacks during take-off and landing. There is limited time for pilots to react in an attempt to prevent collision. Airports are also not designed to ward off drone bombs attacks from the sky.

Following attacks against aircraft in flight, attacks directed at airports were addressed in the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Montreal Convention, 1988 (Montreal Protocol) This protocol criminalizes violence, destruction and disruption at airports.

The biggest challenge in airport security (as well as in other forms of transportation) is the massive influx of people, the majority with luggage. Although luggage may be screened during check-in or before boarding, these steps might be too late in the execution phase of the attack where the airport entrance hall is the intended target. For example, on 22 March 2016, two
brothers executed coordinated attacks targeting transportation infrastructure in Brussels. In the first attack, Brahim el-Bakraoui, and a second suicide bomber, Najim Laachraoui, carried explosives in their suitcases and detonated these at a check-in counter at Brussels Airport in Zaventem, killing 11 people. In the second attack, Khalid el-Bakraoui targeted the Maelbeek metro station in downtown Brussels, in which twenty people died. At least 270 people were injured due to these incidents. ISIS claimed responsibility for the attacks by the two Belgian brothers.58

Countering the terrorist threat at airport entrance halls, Kenya requires passengers to get out of their vehicle approximately two kilometers from the airport building) and go through a metal detector while their hand luggage is scanned through an X-ray machine. The biggest flaw in this system is that after a quick screening of the vehicle by an officer, larger pieces of luggage are allowed to go through unchecked. The use of sniffer dogs to detect explosives could add another layer of security.

Subway and Railway Stations, Trains and Tracks

In comparison to the period 2000 - 2009, attacks against railways and road systems increased between 2010 and 2017 (see Figure 4). Similar to airport security, preventing a potential attacker to enter a bus terminal or train station remains a major challenge. However, in the Shanghai Metro Station, the Chinese government imposed compulsory x-ray screening of all luggage and bags, while also performing random checks of purses at over 700 checkpoints. This has, however, resulted in long queues when the number of entrances to the station was reduced for the purpose of passenger screening.59

Using CCTV and facial recognition can be helpful in identifying and apprehending individuals known to security agencies. But what if the attacker is unknown? The already growing use of artificial intelligence (AI) in the security sector is likely to further increase. According to a report written in 2019, the US Transportation Security Administration (TSA) is engaged in a project that enhances airport security through a Dynamic Aviation Risk Management Solution (DARMS). It is meant to “… integrate information across the aviation sector to tailor a personalized security profile for each person, on a per-flight basis. A smart tunnel will check people’s security while they walk through it, eliminating the need for inefficient security lines.”60 Although implementation is still a few years away, the potential of using a similar system for other transportation systems looks promising. In the UK the
The introduction of trials in 3D scanning of carry-on luggage will no longer require passengers to remove items from bags or limit the amount of liquids taken onboard a plane. With the help of computer tomography (CT), cabin baggage is displayed as 3D rotatable images. Material that could be an explosive is highlighted by color upon which the operator can further investigate the item through studying cross-sectional images. The application of this technology at all airports and beyond will add an important security layer to transportation checkpoints.

The protection against attacks carried out by a passenger on board a train is, however, only one part of the security solution. The other part is determining how to protect tracks against sabotage causing a train to derail. Although not a common feature in Al-Qaeda’s or ISIS’s modus operandi, derailing trains has been a favorite tactic of certain separatist movements. Following a drastic increase in events that included the usage of explosives and obstacles and barriers in since 2016, the Indian government established the Railway Protection Force (RPF) to address this challenge.

Remote Targets

Attacks against the energy and telecommunication infrastructures, being often conducted from a distance, are usually easy to access which increases the likelihood of attacks intended to damage and disrupt such facilities. Although strikes seldom lead to massive casualties, the economic consequences can be severe. It should therefore come as no surprise that the majority of attacks against critical infrastructures are directed against telecommunication facilities and utilities like electricity, oil, and gas lines.

Strikes against energy facilities, including power plants, transmission lines, and generating stations have shown a drastic increase since 2010, with 88 percent of the attackers resorting to explosives as the preferred modus operandi, followed by arson which account for 9 percent of the assaults.

Communication facilities include the Internet, radio, and TV broadcast, telephone facilities as well as other forms of written media (for example newspaper offices). Mobile telephone facilities require special attention, especially in conflict areas, considering the 260% increase in attacks (see Figure 7).

Recognizing that the vulnerability of energy infrastructure increases as a result of being above the ground and therefore visible as well as remote (similar to the telephone network), technological solutions in association with traditional security measures are required as will be briefly discussed in the next section.
Planning for the Worst

The maxim “hope for the best, plan for the worst” applies both in areas constantly targeted, and in areas where there is no prior history of terrorist attacks on infrastructures. Though, from practical experience, it is much harder to convince policymakers to plan for the latter and implement measures against what is regarded as a remote possibility, especially when the cost implications are substantial. It is, therefore, understandable that in addition to the vulnerability assessment of a specific region and the country as a whole, it is crucial to identify areas of special concern which then should be placed on an appropriate level of preparedness. Furthermore, security officials also need to assess the vulnerability of each venue or facility within the broader environment and introduce specific measures to counter and/or minimize the impact an attack might have. The best mental approach in this regard is to plan as if an attack were already in progress, instead of asking oneself whether it could ever happen. With this being said, governments or corporate managements need to be reminded that the success of terrorists rest to a large extent in their ability to surprise and use the unexpected to their advantage as part of their asymmetric warfare. In light of this reality, the following measures and practical steps need to raise awareness and initiate other practical steps to plan and prepare for the worst:

1. Within the framework of a broader threat assessment, management in partnership with security experts need to conduct a risk assessment that identifies key vulnerabilities in- and outside the facility. This is done by identifying: potential routes, traffic flow patterns in and out of the facility, areas where there is a large
concentration of people, times of the day where vulnerability is higher (e.g., rush hour), etc. The overall objective is to develop a layered security solutions design that balances the need for open public access (where required) and concern for public security.

2. Another feature of this framework is the development and implementation of a formal security awareness program. This in turn, ought to be discussed with personnel; in this phase it is also important to ask for the personnel’s input since employees will often present a very different angle to potential risks and vulnerabilities than “outside” assessors. Employees need to understand and accept that their security is both their own responsibility and that of the company or institution. This step is important for informing personnel (especially security personnel) how attacks are planned and what their role is in detecting suspicious activities, most notably during the intelligence collection phase of a planned attack by reporting:
   i) Individuals asking irrelevant questions, for example:
      - An employee at a service center being asked when they open or close is one thing but asking questions around the movement of personnel or other schedules is another.
      - Asking questions about the inside of the building, and the way it was constructed.
   ii) Individuals acting suspicious:
      - Taking “irrelevant” pictures. Today it is extremely easy to take pictures of buildings (with a mobile phone or other device), the positioning of CCTV cameras, fences, and other security measures in place.
      - Potential indicators might include the taking of “selfies” or taking pictures of friends “posing” at the least tourist friendly areas or positions.
      - Strolling might be a sign of boredom but seeing the same person over time in different areas without having a reason to be there needs to be followed up. Algorithms are becoming increasingly available to detect suspicious behavior, including what a person might do next.

3. In addition, it is important to conduct realistic live exercises to develop, implement, and rehearse incident response plans. It is important that these plans should not stagnate but should stay relevant for changing modus operandi and new inventions and trends. Information will empower employees, but it needs to be followed with equipping people with the skills to turn anxiety into preparedness.

Depending on the type of service or facility, proactive measures should take the following key principles – borrowing from basic security – into consideration when developing and implementing dedicated countermeasures. I discuss five below.

*Deter*

These proactive measures reduce attackers’ interest in the target, most notably by means of hardening the target through increasing the risk of being detected prior to an attack (as briefly indicated above) or through implementing measures that will decrease potential success if terrorists should decide on launching an attack. In short, it sways the cost-benefit balance to the negative side.
Detect

These are proactive measures which identify a potential threat through threat, risk, and vulnerability assessments. Using CCTV with facial recognition software to identify individuals acting suspiciously is the most well-known of such measures. The utilization of artificial intelligence (AI) to detect changes in behavior may become a valuable tool in uncovering potential plots during the intelligence collection phase. While CCTV has been useful in the investigation of already executed attacks, for example identifying perpetrators and their movements leading up to an attack – more can be done to prevent attacks through this technology. It will also require a closer relationship between facility-based security personnel and security agencies (especially intelligence agencies) with a clear mandate to investigate potential perpetrators, taking into account privacy considerations of ordinary law-abiding citizens.

Although the majority of high-risk facilities may already have such measures in place, previous attacks on utilities, communication, and transportation systems indicate that remote sites of some of these facilities added to their vulnerability. It is, therefore, necessary to protect the most vulnerable areas during the most likely times attacks occur even in peripheral areas. For example, attacks against mobile phone transmission masts in conflict areas have been a favorite tactic for the Taliban, al-Shabaab, and Maoist militants in India. Telecommunication transmission towers are often easy access targets. If successful, attacks can cause the collapse of telecommunications and further facilitate the operation of terrorist groups in those areas by preventing the public from communicating their whereabouts and movements to security forces. The inability to communicate attacks to security forces allow armed groups to operate with impunity, meaning that by the time security forces are informed attackers have already fled the scene. Similarly, attacks on oil pipelines not only cause environmental damage, but also have a major economic impact, making companies question whether it is viable to remain and/or invest in conflict zones.

It is physically impossible to have enough boots on the ground to protect many telecommunication facilities. Even if security personnel are stationed at such a facility, the possibility of being overrun is real as witnessed in a recent attack in Kenya. On 7 August 2019 in Garissa, Kenya, ten National Police Reservists were kidnapped after the telecommunication mast they were protecting was overrun by suspected al-Shabaab operatives.67

Detecting threats before an attack, purely for the logistical challenges it represents, proves to be extremely difficult. The use of UAVs and other picture/video-based network systems may be useful for identifying attackers, but can usually not prevent attacks and physical intrusions, given reaction times and distances to the scene of an incident. Perimeter Intrusion Detection Systems (PIDS), such as fibre-optic Distributed Acoustic Sensing (DAS) technology hidden below the ground or a pressure sensitive cable or one that builds up an electromagnetic field allow early detection of the footsteps of intruders. Instead of applying this technology within the attack-range of a telecommunication transmitter mast, or an oil or gas pipeline, such a system could be installed at a larger distance from the object to be protected to provide early warning for a timely response. New security systems are able to provide an “acoustic fingerprint” which will allow the system operator to distinguish between people, vehicles, and animals crossing perimeter lines, and also tell him whether a specific activity is occurring (such as digging or fence climbing). This allows them to take the required countermeasures in time to prevent an attack.68

The introduction of UAV technology not only presents a threat to the aviation industry as discussed earlier, but it can also easily be applied to conduct surveillance before launching a ‘traditional type’ attack or launch the actual attack by delivering chemical and biological agents or detonating explosive payloads. With the latter in mind, governments, security companies (commercial), and security agencies (state controlled) need to rethink access control to facilities and other countermeasures. UAV detection and countermeasures has become a
Delay
While early detection will allow the deployment of appropriate countermeasures, additional measures should be in place to delay attackers from reaching their intended goals and gaining access to the target. Physical barriers are most common and include fences, gates etc. These measures need to buy as much time as possible. Over the years, fence technology advanced substantially to include fences that have anti-cut and anti-climb features while some fence and gate types are intended to withstand vehicles. Such crash-rated barrier fences can prevent one or more vehicles from ramming or crashing into a secured facility by absorbing their kinetic energy.

Defense and response capabilities
Depending on the nature of the facility to be protected and the result of threat and risk assessments, high value facilities need to be able to withstand attacks. Even if this self-defense capability will be limited, it should be sufficient until the arrival of reinforcements.

Devalue
All of the above will minimize the impact of an attempted attack, including preventing or at least limiting the number of casualties and the destruction of the facility. This, in turn, will decrease the value of attacking the particular target. When assessing the value of a target, impact on life and limb will be the first criteria, but the impact on the environment (for example an oil spill as a result of a damaged pipeline) and lost income, depending on how long the facility will be inactive, also need to be taken into consideration.

Conclusion
Irrespective of being classified as a “hard” or “soft” target, critical infrastructure will remain in the crosshairs of terrorists as it ticks all the boxes in conveying a message, causing massive casualties or disruption, hurting a country and/or industry economically, attracting massive media attention, and intimidating as many as possible. Considering the diverse nature of potential targets, it is impossible to protect them all. Accurate intelligence about the motives, intentions, and capacities of the adversary is necessary to prioritize preparations. Yet, those responsible for protecting infrastructure against terrorist attacks need to plan also for less probable scenarios - not only by considering what happened in the past (and being reactive), but also by considering what is likely to happen in the future (and being proactive). Possible countermeasures can be expensive, but policymakers should keep in mind that these countermeasures can often also be applied for preventing and countering natural disasters and man-made non-terrorist accidents.

This chapter started by explaining the concept of “critical infrastructure” and how it relates to the overall aim of terrorists to attack associated sector facilities. Specific reference was made
to the OAU’s categorization of intent by targeting “public or private property, natural resources, and environmental or cultural heritage.”

The second part of the chapter emphasized the need to conduct periodic threat-, risk-, and vulnerability assessments to be continuously abreast and prepared for potential threats, especially since attacks seldom take place outside situational developments within a particular time and place. While the purpose of assessment analysis needs to be clear, those responsible need to constantly keep the purpose of attacking critical infrastructure in mind. In other words, what makes a country’s critical infrastructure attractive to attack? Taking into consideration that the planning of such attacks requires a basic cost-benefit analysis: those tasked with preventing and countering acts of terrorism and sabotage need to increase the cost of attacking a particular facility or sector, while decreasing the benefit the group or organization may attain from executing the attack(s).

Shedding light on the type of threats critical infrastructure may potentially have to deal with, this section of the chapter tried to explain future modi operandi and target selection by highlighting previous incidents. Furthermore, specific reference was made to the transportation industry, (most notably airports and airplanes, and the railways), utilities (electricity, gas, and oil networks and facilities), and the communication infrastructure. The use of UAVs, drones, and SAM/MANPADS were briefly highlighted as their use requires additional and specific countermeasures.

Anneli Botha is a Senior Lecturer at the Department Political Studies and Governance at the University of the Free State in Bloemfontein, South Africa. She also serves as an independent consultant on radicalization, deradicalization, reintegration and terrorism in Africa. In the period 2003 – 2016, she worked as a senior researcher on terrorism at the Institute for Security Studies (ISS) in Pretoria, South Africa. She has travelled extensively throughout Africa where she conducted research on terrorism and delivered specialized training on various aspects of the threat of terrorism, extremism, radicalization and counter-terrorism to law enforcement and criminal justice officials on the continent. Prior to her position at the ISS, she served in the South African Police Service (SAPS) for 10 years. Highlights included being a founding member of the Religious Extremism and Terrorism Desk at the Crime Intelligence Head Office and serving in the Rapid Reaction Unit and the Special Task Force on Urban Terror in the West Cape. At the end of her police career she provided strategic support to the Head of South Africa’s Crime Intelligence Unit. Anneli Botha holds a Magister Artium degree from Rand Afrikaans University in Political Studies (1998) and Philosophiae Doctor from the Department of Political Studies and Governance at the University of the Free State (2014). Her award-winning Ph.D. thesis was titled: “Radicalization to Commit Terrorism from a Political Socialization Perspective in Kenya and Uganda.” Additionally, she is a graduate of the University of Pretoria, Political Science (1991) and International Politics (1992).
Endnote


17 Literary Devices. Symbolism. Available at: https://literarydevices.net/symbolism/


29 Ibid., p. 48.

30 Based on information obtained from the National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, University of Maryland. Available at: https://www.start.umd.edu/gtd/

31 Ibid.


36 Data obtained from National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, College Park: University of Maryland. Available at: https://www.start.umd.edu/gtd/
37 Laville, Sandra, ‘Five Key Questions for Anti-Terror Investigation’, The Guardian, 19 August 2006. Available at: https://www.theguardian.com/uk/2006/aug/19/terrorism.world
51 Hudson Bernard, ‘Drone Attacks are Essentially Terrorism by Joystick’, Washington Post, 5 August 2018. Available at: https://www.washingtonpost.com/opinions/drone-attacks-are-
essentially-terrorism-by-joystick/2018/08/05/f93ec18a-98d5-11e8-843b-36e177f081e_story.html?utm_term=.44fab7a35c53
54 Coulter Martin and Naomi Rovnick, ‘How Big a Threat are Drones at Airports?’ Financial Times, 20 December 2018. Available at: https://www.ft.com/content/ee9bb576-0455-11e9-99df-6183d3002ee1
57 Data obtained from National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, College Park: University of Maryland. Available at: https://www.start.umd.edu/gtd/
61 Data obtained from National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, College Park: University of Maryland. Available at: https://www.start.umd.edu/gtd/
64 Data obtained from National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, College Park: University of Maryland. Available at: https://www.start.umd.edu/gtd/
65 Ibid.


69 DroneShield, *Detect. Assess. Respond*. Available at: https://www.droneshield.com/


Bibliography


Coulter, M and Rovnick, N., ‘How Big a Threat are Drones at Airports?’ Financial Times, 20 December 2018. Available at: https://www.ft.com/content/ee9bb576-0455-11e9-99df-6183d3002e1


DroneShield, Detect. Assess. Respond. Available at: https://www.droneshield.com/


Louw, P. E., Literary Devices, Symbolism. Available at: https://literarydevices.net/symbolism/


Web-based Resources

Clarion Project, Islamic State’s (ISIS, ISIL) Magazines. Available at: 
https://clarionproject.org/islamic-state-isis-isil-propaganda-magazine-dabiq-50/
Jihadology, a clearing house for Jihadi source material. Available at: https://jihadology.net/
National Consortium for the Study of Terrorism and Responses to Terrorism: Global 
Terrorism Database, University of Maryland. Available at: 
https://www.start.umd.edu/gtd/
The Quality Infrastructure Investment Database, An initiative of the G20 under the 2019 
Japanese Presidency, in collaboration with the Global Infrastructure Hub, the OECD and 
the World Bank. Available at: https://www.gihub.org/quality-infrastructure-database/
US Homeland Security, Critical Infrastructure Security. Available at: 
https://www.dhs.gov/topic/critical-infrastructure-security
Chapter 29

Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness

With Three Case Studies on Estonia, Singapore, and the United States

Shashi Jayakumar

The field of cyberterrorism has existed for as long as it has been possible to interdict or compromise computer systems. While contributions of scholars, researchers, and practitioners have enriched discussions, there are longstanding and unresolved issues of definition which can give rise to confusion. Does cyberterrorism mean attacks only by individuals groups that fall within widely accepted definitions of “terrorist” or “terrorist organizations?” To what degree does the aim or intention of the malicious actor matter? For the purposes of the present volume, this study (without sidestepping these questions) examines attacks against computer infrastructure and Critical Information Infrastructure (CII) by all actors with capability, and not just groups such as Al-Qaeda or ISIS. As the author notes and establishes early in his discussion, this is necessary given that while conventional terrorist groups might have intent, they have not to date acquired the capability to carry out a genuinely destructive cyber-attack of the type that might lead to major loss of life or infrastructural damage. It is (for the most part) states which have this capability. Cyber prevention and preparedness covers a wide range. This three-part chapter includes technical aspects of cyber protection, systems (and people) resilience, risk mitigation, as well as nurturing talent within a viable cyber ecosystem. Three case studies (Estonia, Singapore, and the US) are given where these and other relevant issues are examined.

Keywords: advanced persistent threat, cyber, cyberattacks, critical information infrastructure, cyberterrorism, hacking, malware, phishing, Supervisory Control and Data Acquisition, industrial control systems
Meaning of “Cyberterrorism:” Past, Present, and Future

What is cyberterrorism? Is cyberterrorism simply terrorist acts (causing death, serious disruption, fear in the target population, attempting to change the ideology of a people) carried out using digital or cyber electronic means, or does it involve cyberattacks carried out by terrorists and terrorist groups? Does the actor actually matter? Can cyberterrorism technically speaking be done by a state?

In 1997 Mark Pollitt, special agent for the FBI, offered an early working definition of cyberterrorism: “Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents.”

It is tempting, following Pollitt’s influential - and early - attempt at definition, to simply suggest that cyberterrorism can only be committed by what are considered terrorist organizations (that is, non-state actors or the clandestine agents highlighted by Pollitt). But consider another relatively early, and still useful definition from James Lewis, who in 2002 defined cyberterrorism as “the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.” Lewis’ definition is similar in some respects to Pollitt’s, but Lewis leaves open the possibility that state action might be caught within his definition as well.

Finally, consider a widely-cited definition by Dorothy Denning:

“Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.”

Denning is precise when it comes to what types of acts constitute cyberattacks, and, like Lewis, is actor-agnostic: her definition leaves open the possibility that actors apart from conventional non-state terrorist groups and organizations might be caught.

Past surveys of experts aimed at either arriving at definitions of cyberterrorism (or indeed aimed at elicting views on whether a definition is necessary) tend to have shown more than anything else that there is no single accepted definition; nor is there likely to be one in the near future. This chapter avoids tendentious discussions on contested definitions of cyberterrorism; nor for that matter has this author chosen to dwell on the vexed question as to whether or not all cyberattacks are cyberterrorism attacks. The first part of this chapter is a discussion of cyberattacks by what are conventionally understood as terrorist organizations. Following this, in the second part of the chapter the discussion is broadened to study cyberattacks by malevolent actors. These could be state and non-state actors; necessarily, the instruments could be used by terrorist groups or individuals. Preparedness against, and prevention of, cyberattacks are then discussed with three case studies (the US, Estonia, and Singapore) in the third and final part of this chapter.
Cyber Attacks by Terrorist Organizations

Cyber-attack plotting by terrorist organizations has a long history. This section discusses two periods: the late 1990s to early 2000s where cyber-attacks were largely aspired to, to early 2000s to 2015 when intent became more visible.

1990s – 2000s: Aspiration

Terrorist groups such as Al-Qaeda have had a presence on online platforms since the late 1990s. Using the internet was (and is) cheap and (relatively) anonymous; it also bypassed mainstream or traditional news sources with the websites and forums, certainly in the earlier phase, largely free from any meaningful censorship. This route also provided the means to quickly reach a growing audience.

Al-Qaeda’s leadership had, from early on, a vision of attacking Western critical infrastructures, and it does seem that this vision could have encompassed remote attacks by computer or digital means. This aspirational goal devolved in time to the wider Al-Qaeda-sympathetic diaspora, members of which would, from time to time in the 2000s, make claims on various online platforms concerning the development of cyber/hacking capabilities and impending cyber-attacks (such as DDoS attacks). In general, these either never materialized or were markedly unsuccessful.

From time to time, individuals who claimed some sort of affiliation or link to Al-Qaeda would gain something of a reputation for hacking prowess. An example was Younis Tsouli, who became infamous as “Irhabi 007” (“Terrorist 007”) from 2003 until his arrest a few years later. Starting out in various extremist forums where he uploaded instruction manuals on computer hacking, he began to support online operations linked to Al-Qaeda, and in 2005 became the administrator of the extremist internet forum al-Ansar. Tsouli’s actual hacking ability appears to have been moderate at best, but by the time of his arrest by October 2005 he had gained a wide reputation as a hacker of some prowess, as well as having the ability to securely distribute across the internet Al-Qaeda’s messages.

2000s – 2015: Intent

From the early to mid-2000s, governments, analysts, and observers began to have a heightened appreciation of how terrorist organizations (such as Al-Qaeda and Hezbollah) were becoming more adept in their understanding of the possibilities that the internet and digital technologies afforded them, and how this could in turn lead to a mastery of the tools needed for a successful cyber-attack.

In 2011, an Al-Qaeda video called on followers and sympathizers to launch cyberattacks against Western targets. The video, which came to public attention the following year, apparently observed that the US was vulnerable to cyberattacks, just as airline security was vulnerable in 2001 in the period leading up to the 9/11 attacks. The video called on Muslims “with expertise in this domain to target the websites and information systems of big companies and government agencies.” However, no cyberattack from Al-Qaeda Central ever seems to have materialized.

There was an uptick in interest, and in the number of groups themselves, after the declaration of the Caliphate in 2014. ISIS, as well as various pro-ISIS influencers and cheerleaders were keen in disseminating key texts online, or dispense advice to jihadi aspirants, through various online means, including (besides mainstream online platforms) encrypted messaging apps such as Telegram, which have become increasingly popular, notwithstanding recent crackdowns by Telegram itself and by national governments. Needless to say, these platforms and apps were instrumental for many individuals on various points of their
radicalization journey to meet each other virtually, exchanging views and information, and, through this discourse, further influencing or reinforcing each other’s beliefs. Further, there is evidence that plotting of terrorist attacks has increasingly taken place on social media, encrypted messaging apps, or the “Dark Web.” In some cases, the perpetrator can be guided “remote-controlled,” as it were, by an overseas mastermind, sometimes in near real-time. These areas have become an increasing focus of concern for security agencies.

While various ISIS media units have been successful in disseminating messages and slickly-produced propaganda online, the lack of genuine cyber disruptive capability could be said to have continued on into the ISIS era. Threats of hacking were not altogether infrequent. On 11 May 2015, Rabitat Al-Ansar, a pro-ISIS collective, released a video titled, “Message to America: from the Earth to the Digital World,” threatening hacking attacks against American and European targets. The following year, it tweeted plans to hack US targets, including government websites on 11 September 2015; these appear not to have materialized.

At an individual level, ISIS members or individuals with pronounced pro-ISIS sympathies did have some technical knowledge of the type to create basic attacks, and, in some cases, were able to co-opt cadres of like-minded individuals to attempt attacks. A prime example is Junaid Hussain Abu Hussain al-Britani, a UK national who went to Syria in 2013. Prior to his move, he appears to have been a hacktivist with allegiance to various causes (including the Palestinian cause, and against far-right groups in the UK; an illustration of the point that the line between hacktivism and cyberterrorism may sometimes be not all that clear-cut), as well as associating with well-known hacking collectives such as Anonymous. He also founded “Team Poison,” responsible for hacking NATO, and the British Ministry of Defense. He was jailed in 2012, with his incarcerations playing some part in hardening his views. After his release, he resurfaced in Syria, becoming not simply a key ISIS influencer on Twitter, but, it appears, an important member of ISIS’ cyber offensive operations team. During this time Junaid attempted attacks against various websites linked either directly or indirectly with the anti-ISIS coalition (or against countries that supported anti-ISIS efforts).

Other pro-ISIS elements have had basic hacking and data exfiltration ability. In 2016, Ardit Ferizi, originally from Kosovo, became the first person ever prosecuted in the US on cyberterrorism charges, in a case that, according to US officials, represented “the nexus of the terror and the cyber threats.” Ferizi (who was sentenced to 20 years imprisonment), went online by the moniker Th3Dir3ctorY, was arrested in Malaysia (where he had been studying computer science) in October 2015. According to the US federal criminal complaint filed against him, Ferizi and his associates stole the personal information of more than 1,300 US military and government personnel through hacking an unnamed US company. This personal information was then passed to Junaid Hussain, who, in the name of the Islamic State Hacking Division (ISHD), released details of these individuals in August 2015 - the same month that saw him killed in a drone strike. The publication of the “kill list” was something of a minor propaganda coup. But some of Hussain’s “kill list” releases were actually not hacks nor the exfiltration of data, but detailed open source research. Indeed, in the recent history of doxing and the release of kill lists, the sense is that these were not highly sophisticated attacks, with some of these releases involving (essentially) repackaged information available elsewhere. A case in point was the January 2015 hack of the CENTCOM (US Central Command) Twitter and YouTube pages. Besides posting threatening messages against the US on the pages, what appeared to be US military documents (although not classified) were released. This was not a hack into a sensitive military network, and was characterized (although something of a propaganda coup by the perpetrators, who may have included Junaid Hussain) as “cyber-vandalism.” by US authorities.

Pro-ISIS online groups such as the United Cyber Caliphate have continued what could be best described as low-level hacks, attempting DDoS attacks in 2016 and 2017. The attacks were mainly focused on targets in the Middle East, and although some of the targeted sites
appear to have been briefly knocked offline, the action points more towards a kind of resourcefulness rather than a high level of technical mastery. 24 Separately, hackers sympathetic to some degree to ISIS – in this case the group known as the Tunisian Fallaga Team – carried out a series of attacks against the UK’s National Health Service (NHS) – involving defacing websites to show gruesome images of the Syrian Civil War. 25

Overall, the cyber offensive ability of groups conventionally thought of as terrorist organizations (such as Al-Qaeda or ISIS) should be considered to be of a fairly basic order, with no compelling evidence that these groups have been able to launch a full-scale cyber-attack of the type that causes harm, death, or destruction, or which has instilled fear in the population of a country. 26 While concern over potential cyberattacks has grown in recent years, commensurate with the growth in digital and cyber infrastructure, the vast majority of serious attacks that have caused either serious damage or disruption (or monetary loss) can be traced to criminal organizations, or states, but not to terrorist organizations. It is states, for the most part, who up till this point of time have a serious capability in the cyber sphere to cause destruction through cyber/digital means. 27

The remainder of this chapter does not confine itself to what governments and the private sector have done to protect against attacks by terrorist groups or subnational groups. Good prevention and preparedness does not by its very nature attempt to distinguish who the malicious actor is, and national preparedness has to be premised facing major threats first, whatever their origin. As Gen. John Gordon, Assistant Secretary for Intelligence at DHS (also at the time serving as chairman of the Homeland Security Council), observed at the RSA Conference in 2004, “The damage will be the same whether the attacker was a bored teenager, an organized criminal or a [hostile] nation or state. We need to focus on the vulnerabilities—and not get too hung up on who the attacker will be.” 28

**Cyber Attacks by Malevolent Actors**

While terrorist groups lack the ability to severely impair the operations of state machinery, technologically advanced states with resources and developed cyber offensive capabilities can (given time and planning) severely impact terrorist organizations through cyberattacks (for a sense of what the various actors are capable of, see Figure 1). In 2016, the US Cyber Command and the National Security Agency commenced a major cyber operation, Glowing Symphony, which severely impacted ISIS’ media operations. 29 In a separate operation from the same year, cyber operatives from the Australian Signals Directorate hacked into ISIS communications thousands of miles away, interdicting ISIS communications, directly assisting anti-ISIS coalition forces about to launch a major operation. 30

In the pursuit of national objectives, states – and for the time being states alone - can deploy cyber weapons capable of physical damage. In the earlier era, assumptions on hacking and computer network attacks tended to take into account compromises of computers or networks (“disruptive” activity), assuming that critical infrastructures were less vulnerable as they were far more difficult to penetrate. 31 These assessments for the 1990s and most of the early 2000s were correct at that time, but events in recent years have shown that this assessment can no longer be regarded as tenable. As computer networks have become increasingly enmeshed with critical infrastructure, corresponding vulnerabilities have multiplied. This means that the attack surface has grown dramatically in recent years. One of the earliest cyberattacks that caused physical damage is Stuxnet, a malware which was responsible for causing damage at the Iranian uranium enrichment facility in Natanz between 2009 and 2010. 32 Stuxnet is commonly agreed by experts to have been the joint creation of the security services of the US and Israel (although both countries have not officially accepted responsibility).
Figure 1. Cyber Attacks from Actor to Aim

<table>
<thead>
<tr>
<th>Actor</th>
<th>Target</th>
<th>Attack mode</th>
<th>(Primary) Aim/ Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Warfare</td>
<td>• States</td>
<td>• Military and civilian infrastructure, CII (critical information infrastructure)</td>
<td>• Force surrender; • Negotiated settlement on favorable terms • Degrade opposing side’s ability in peacetime/prior to commencement of declared hostilities • Subversion/undermine resilience of target</td>
</tr>
<tr>
<td></td>
<td>• Private sector</td>
<td>• Private Sector (ICS, SCADA systems)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Civilians</td>
<td>• Social engineering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Government institutions</td>
<td>• Phishing attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Terrorist groups and non-state actors</td>
<td>• Watering hole attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IOT attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Botnet Attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disinformation campaigns/ influence operations/attacks against election system</td>
<td></td>
</tr>
<tr>
<td>Cyber Espionage</td>
<td>• States</td>
<td>• State infrastructure/military-industrial complex</td>
<td>• Theft of intellectual property / commercially sensitive or valuable information</td>
</tr>
<tr>
<td></td>
<td>• Private sector</td>
<td>• APTs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ICS, SCADA systems</td>
<td>• Data exfiltration</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Social engineering</td>
<td></td>
</tr>
<tr>
<td>Cyber Crime</td>
<td>• Criminal groups (including criminal groups acting on behest of states);</td>
<td>• State infrastructure</td>
<td>• Financial gain</td>
</tr>
<tr>
<td></td>
<td>• States</td>
<td>• Private sector</td>
<td></td>
</tr>
<tr>
<td>Ideological/ Cause-based attacks/ Hacktivism</td>
<td>• Extremist /anti-establishment groups; Black Hat hackers</td>
<td>• Malware (including ransomware) • APT • Social engineering • Phishing attacks • Watering hole attacks • IOT attacks • Botnet attacks</td>
<td>• Force political /social change • Sow fear in target population</td>
</tr>
<tr>
<td></td>
<td>• States</td>
<td>• DDoS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Private sector</td>
<td>• Phishing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Basic malware</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Defacing websites</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Doxing</td>
<td></td>
</tr>
</tbody>
</table>
Computer malware can cause physical damage and potentially loss of life (even though the latter has not yet happened). In recent years, analysts therefore have been forced to treat malware-based attacks against critical infrastructure (including ICS (Industrial Control and SCADA (Supervisory Control and Data Acquisition) systems as a serious cyber threat.

Another case in point is an attack against an unnamed steel mill in Germany that occurred, it appears, sometime in or just before 2014. The malware affected the operations of a blast furnace, causing a great deal of (unspecified) damage. The malicious actor, not formally named, deployed tolls and showed skills of a high level. These included a combination of spear phishing, social engineering methods aimed at particular individuals, as well as familiarity with the not just conventional IT security systems but also mill’s specialized control systems.

Many cyberattacks fall just short of those described above in terms of severity (or immediacy) but still have a serious fallout. Saudi Aramco, the state petroleum and natural gas company of Saudi Arabia, was hit by a major cyberattack in August 2012 that affected 30,000 workstations. Critical files were overwritten with an image of a burning American flag. A group “Cutting Sword of Justice” claimed the attack was in retaliation for the Saudi regime’s “crimes and atrocities taking place in various countries around the world.” The malware had a data wiping capability, and could thus be considered destructive to some degree as opposed to simple DDoS style attacks. The attack was seen by some as a hacktivist attack, but state responsibility (possibly Iran) cannot be ruled out.

Some cyberattacks exhibit more aspects of reconnaissance, probing vulnerabilities, or deployment of assets in advance of (or in preparation for) the outbreak of hostilities. From around 2016, for example, there began to be reports of Russian attempts to probe the US power grid. No physical damage was caused, and the probing appears to have been more of a sniff out vulnerabilities operation. The US appears to have returned the favor, with evidence suggesting that relevant agencies have begun in recent years to aggressively intensify existing efforts to probe and implant malware in the Russian power grid.

Government control over their cyberweapon creations is not fool proof: malware that is kept for use at a later date (or else meant for a specific use) can escape “into the wild” and be used by others. An example is the EternalBlue exploit, allegedly stolen from the National Security Agency (NSA) in 2016 and leaked online in April 2017 by a group known as Shadow Brokers. This, in turn, enabled high profile cyberattacks, including the infamous WannaCry attacks, used by states as well as cybercriminals, as well as the 2017 NotPetya malware campaign, which crippled parts of the Ukrainian government (an attack thought to have been executed by the Russian military) before spreading to multinational corporations such as FedEx and Maersk, causing billions in damage.

Certain states that might be considered “rogue” nations might attempt cyber offensive methods that are more commonly associated with criminal enterprises. North Korea, for example, is thought to have been responsible for a string of attacks against various state and non-state targets. Its activities in recent years have included cyber theft and attacks against the international banking system. These attacks, which included hacks against cryptocurrency exchanges, generated income to fund, inter alia, North Korea’s nuclear program. These hacks also included attacks against the international banking system through the exploitation of weaknesses of the SWIFT payments system, most notably a February 2016 heist which saw the theft of $81 million from the account of the Bangladesh Central Bank at the Federal Reserve Bank of New York. APT 38, a group linked to the North Korean regime, is thought to be responsible, and has also been linked to cyber heists targeting numerous other financial institutions.

When states undertake a course of offensive cyber action, there are often “guardrails” that might prevent collateral damage. The malware might, for instance, have an expiration date, or else it might be precisely tailored and only usable in certain locations and contexts. But states that occasionally exhibit “rogue” cyber behavior do not exhibit such guardrails, with the
malware either capable of causing indiscriminate damage, or the attack itself designed to be visible and to embarrass or draw attention to the attack or the target. The well-known cyber hack against Sony Pictures, allegedly carried out by North Korea in 2014, is a case in point, with confidential Sony documents posted online by the hackers.\textsuperscript{45}

Cyber strikes may be carried out by states in retaliation for certain actions. In the wake of the drone and missile attacks against Saudi oil processing facilities in Abqaiq and Khurais on 14 September 2019, for example, reports suggested that the US carried out a retaliatory cyber strike against Iran, the country which was widely thought to have been behind the attack on Saudi Arabia. This cyber strike was severe enough to affect physical hardware.\textsuperscript{46} The US also appears to have carried out a cyberattack in June 2019 against Iranian maritime installations, partly as retaliation for attacks in May and June 2019 against shipping in the Gulf of Oman and the Persian Gulf, and the destruction of a US drone by an Iranian missile on 20 June 2019.\textsuperscript{47}

States with advanced capabilities routinely engage in cyber espionage and theft of intellectual property as well. An example of an APT group linked to a series of hacks attempting to steal intellectual property and industrial secrets is APT 10/Cloudhopper, which has been linked to the Chinese Ministry of State Security (MSS).\textsuperscript{48} The cyberattack against the Norwegian software firm Visma in 2018 which saw client information stolen also appears to have been carried out by hackers working on behalf of the Chinese state security apparatus (part of a wider, organized campaign.).\textsuperscript{49} In the US in particular, there has, in recent years, been considerable discussion and public debate about the scale of intellectual property theft conducted by China, with then-National Security Agency Director and Commander of Cyber Command Keith Alexander calling this in 2012 “the greatest transfer of wealth in history.”\textsuperscript{50}

As events of recent years have shown, some states are willing and able to attack other states using cyber means (hacking) combined with social media manipulation, information warfare, troll farms, hackers, and cyber espionage operating in a mesh. The aim can be to undermine the resilience of a country, to humiliate it, or to influence the course of the democratic process. Although a full treatment would be beyond the scope of this chapter, it is worth at this point to consider briefly Russian interference in the 2016 presidential election in the US. One prong of this interference involved subversion and the creation of fake groups on social media to sow dissension in society. Another prong involved hacks and subsequent publishing of stolen material from the Democratic National Committee’s servers in 2015 and 2016, by (it appears) more than one group linked to Russian intelligence services.\textsuperscript{51} One of the groups involved, Fancy Bear (or APT 28), which has been linked to GRU, Russia’s military intelligence agency, is thought to be responsible for the 2015 hack of the German Bundestag.\textsuperscript{52} German officials were clear that the Russian state could, if it wished, release the exfiltrated messages in the form of doxed material or for disinformation purposes, or to damage the integrity of the German elections.\textsuperscript{53} The same group has been identified as being behind the attempted interference (through the exfiltration and publication of emails) in the 2017 election campaign of presidential candidate Emmanuel Macron.\textsuperscript{54}

Finally, activity by criminal or hacktivist elements not linked to states also needs to be considered. In recent years, cybercriminals have in recent years been capable of causing a type of severe impairment which - while not amounting to physical damage - can still hinder certain types of operations. In March 2018, for example, Atlanta’s municipal administration (including government departments and the police records system) was severely affected by ransomware attacks using the SamSam virus which saw the administration of this American city spend over $2.5 million to regain control.\textsuperscript{55} In addition to the financial sector, in recent years the healthcare sector has also increasingly come into the crosshairs of criminal enterprises. Theft of data (including research data) and personal information can be very lucrative, as the data can be used for identity theft and can be resold on the Dark Web. Increasingly, a particular risk area for healthcare has been the use of Internet-of-Things (IOT) -enabled devices (such as pacemakers) which can be compromised.\textsuperscript{56} More generally, it appears to be just a matter of
time before the nascent IOT is compromised in other sectors as well. While some of the methods themselves are not yet firmly in place, there is evidence that the criminal underground is on the lookout for ways to refine its approaches in this respect.\textsuperscript{57} Individual hackers or small hacker collectives have not yet reached a level capable of causing serious disruption or major monetary loss, but their activities have on occasion garnered attention from media and law enforcement. A case in point is LulzSec, a loose hacker collective with a small group of members which was behind various hacks in 2011. LulzSec’s activities included attacks against Fox Broadcasting, Britain’s National Health Service (NHS), and Sony Pictures (attacks included gaining access to administrator passwords, causing website outages, and accessing customer details). Law enforcement in the UK and the US took action and some of the members were arrested and charged.\textsuperscript{58} There have been occasions where the actions of individual actors or small groups have had an outsized effect on ICT infrastructure. One example is the Mirai botnet, created in 2016 by three college-age students in the US, for no greater purpose than trying to gain an advantage in the online game Minecraft. Mirai eventually escaped into the wider online world, taking control of a huge number of other computers and IOT-enabled devices. Together with the various variants it spawned, it was from October 2016 to early 2017 responsible for over 15,000 individual DDoS attacks, and for a time affected the internet in the Eastern US.\textsuperscript{59}

**Part II: Four Tiers of Preparedness and Prevention**

“We will be in a world of ceaseless and pervasive cyber insecurity and cyber-conflict against nation-states, businesses and individuals.”

- Glenn S. Gerstell, General Counsel, National Security Agency, September 2019\textsuperscript{60}

This section will discuss the four tiers of preparedness and prevention: international cooperation; government; private sector; and the public.

1. **International Level**

In the past, there have been global (or regional) efforts to strengthen cooperation on cyber issues through treaties and international agreements. An example is the Convention on Cybercrime, commonly known as the Budapest Convention, which entered into force in 2004.\textsuperscript{61} The Convention covers (inter alia) information sharing and mutual assistance, as well as developing a common framework for tackling cybercrime, including interference into computer and ICT systems.

Efforts like the Budapest Convention might be considered useful beginnings, but the critical issues within the global cyber debate continue to be argued over, with key protagonists unable to reach agreement on what exactly constitutes cyber conflict (and what level of cyber operations qualify as “use of force” or “attack”), whether the law of armed conflict applies in cyberspace, and what constitutes acceptable state behavior in cyberspace both in times of conflict and peace, and what constitutes acceptable and proportional response to a cyber-attack.\textsuperscript{62} Academics and experts have from time to time made efforts to come up with (necessarily non-binding) manuals on these issues.\textsuperscript{63} While some of these efforts have been well-received, they have had limited real-world effect. The same may be said of efforts by
individual governments – even well-regarded ones which have done considerable thinking on these issues – to set out national positions on some of these very problem-fraught issues.\textsuperscript{64}

It is no accident that some of the key norm-shaping mechanisms have been conceived under the ambit of the UN. The UN Secretary-General António Guterres himself has on several occasions expressed concern over the use of cyber means for malicious purposes, noting that cyberattacks had contributed to diminishing trust among states.\textsuperscript{65} Cyber features prominently in the UN’s Agenda for Disarmament, especially when it comes to promoting responsible behavior and ensuring peace and stability in cyberspace.\textsuperscript{66} There are, at the time of the writing of this chapter, within the UN two separate ongoing deliberative processes that are ongoing – the UN Group of Governmental Experts (GGE) and the UN Open-Ended Working Group (OEWG). Both seek to address the issue of promoting responsible state behavior in cyberspace.\textsuperscript{67}

A full discussion on global debates on international norms, rules of the road, and acceptable state behavior falls beyond the scope of this chapter. However, it can be observed here that amidst ambiguity and lack of settled consensus on norms, some powers could be said to have already entered into a state of \textit{undeclared} cyber warfare – activity that is usually deniable (or denied) and calibrated to stop just short of the level that might invite an armed response or a declaration of hostilities in the physical world.\textsuperscript{68} Given this reality, and given the absence of any likelihood of global agreement on acceptable behavior in cyberspace, governments themselves, depending on national contexts, often have had to take the overall lead in securing sovereign cyber defenses. The private sector (given the risks of damaging hacks, ransomware and IP theft) has also begun to pay considerably more attention to cybersecurity than in the past.

Finally, good cyber hygiene and preparedness at the level of the individual has also been increasingly emphasized by experts and governments as the cornerstone of cyber resilience.

2. Government/National Level – The Cyber Ecosystem

As we increasingly become networked at a personal level, and as the economic foundations of states are increasingly tied to digital infrastructure and the digital economy, governments, corporations, individuals and national (as well as international) ICT infrastructures face an enormous range of threats. These span from state actions almost amounting to cyberwarfare to hacking, espionage (which can involve the theft of secrets and IP), to botnets created for various purposes.

That is just the present. With an unavoidable future of information technology ever more embedded in our everyday lives, plus the promise – and peril – of the Internet of Things (IOT), cyber threats that did not exist in a not-so distant past are now moving from the realms of the conceptual into concrete emergent threats. The intensification of the threat should not therefore be measured solely in terms of numbers of malware attacks; the diversification of the malware itself and evolution of hackers’ methods bear watching.\textsuperscript{69}

The use of Artificial Intelligence (AI) in cyberattacks is a case in point. Experts note that conceptual models for AI-powered attacks (for example, to evade anti-virus mechanisms, or to crack passwords) exist and can be used to strengthen existing malware.\textsuperscript{70} There have already been cases of voice “deepfakes” used to trick unsuspecting company employees to make payments to fraudulent accounts (by using AI to convincingly spoof the voice of the CEO or senior company official).\textsuperscript{71}

The cyber environment is therefore by default a compromised one. Cybersecurity has had to become much more than simply the state or its constituent parts repelling attacks. Governments and corporations alike have increasingly come to acknowledge that cybersecurity paradigms envisaging complete protection, and all attacks repelled, is chimerical. Rather than focusing on absolute prevention, or trying to achieve a “good” level of cybersecurity, some of
the most practical – not to mention sensible - approaches emphasize overall risk mitigation, minimizing the impact of cyber intrusions, and defense-in-depth to enable systems continuity.\textsuperscript{72} In practice, this means a shift in focus toward cyber resilience, which the US National Institute of Standards and Technology, has usefully defined as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”\textsuperscript{73}

One aspect of resilience and overall risk management has to do with technical approaches and systems engineering. This might involve regular systems upgrades and building in of specific redundancies and back-ups with the system. These should not be treated as an afterthought: the systems that are genuinely cyber resilient are those which have these security features and redundancies built into the architecture from the design stage. If done correctly, the mission-critical functions of an enterprise will be better able to withstand cyberattacks, respond adaptively, and also operate even when compromised to some degree.\textsuperscript{74} States that have considered the issue deeply, however, assess that cyber resilience is not simply a technical or engineering competence. High-level direction and decision, as well as a comprehensive vision, is necessary in order to communicate national objectives in the cyber domain.\textsuperscript{75} Increasingly, this has come in the guise of holistic cyber security strategies or masterplans. These might encompass (for example) robustness (containing threats and repelling them), resilience (which either at the government or private sector level might involve mitigation, sharing information, public education), and other aspects of defense (early warning, deterrence), with these three factors being interdependent.\textsuperscript{76} By the end of 2018, over 90 countries had such a strategy.\textsuperscript{77} The actual content however varies from country to country: Finland’s Cyber Security Strategy has three main prongs: the development of international cooperation, better coordination of cybersecurity management, planning and preparedness of cyber security and the development of cyber security competence and skills, while the four pillars of Singapore’s Cybersecurity Strategy pertain to resilient infrastructure(s), a safer cyberspace, a vibrant cybersecurity ecosystem, and strong international partnerships.\textsuperscript{78}

Government has a critical role in instilling a mindset and culture of cybersecurity throughout all levels of society. It also sets standards (e.g. through regulation), and ensures accountability. Transparency at all levels (government, the private sector, and the public at large) is critical in order for relevant agencies to obtain a holistic threat picture. Several nations have thus introduced within their cyber legislation or frameworks mandatory reporting of cyber breaches – especially breaches that cross a certain threshold of severity. Australia, for example, made it a legal requirement through its Notifiable Data Breaches Scheme in 2017 for organizations to notify individuals as soon as practicable when their personal information is involved in a data breach that is likely to result in “serious harm.”\textsuperscript{79} Typically, overarching cyber legislation extends to cover the private sector, with governments assessing that cybersecurity is a public good that cannot be provided by the market. A further calculation is that it is unsatisfactory to allow cybersecurity standards to be left to the private sector (which might see cybersecurity primarily as a cost item, or which might lack incentives to invest in cybersecurity) to decide.\textsuperscript{80}

At the heart of national cyber defenses, in terms of operational readiness, ought to be a Computer Emergency Response Team (CERT). Ideally, this should be much more than a team of technical experts attempting to defeat malware attacks. Although the core work of CERTs involves minimizing the risks and effects of cyberattacks, effective CERTs look holistically at the cyber threat surface and mitigation efforts: these might involve data security, endpoint security, testing and national (or sector-specific) cyber drills.

Near the top of state/CERT priorities for cyber defense has to be the protection of critical information infrastructures (CII) – computer systems directly involved in the provision of essential services. Examples might be the power grid, telecommunications services or the banking system. CII are complex and often interdependent, and the prospect of a sophisticated
cyberattack crippling CII (potentially with knock on effects cascading through the economy and through other sectors) has now become a tangible threat.\textsuperscript{81} It is on account of this that national cybersecurity exercises for key CII are a regular occurrence for states which prioritize cybersecurity. Besides multi agency involvement from the government, the best of these exercises bring in the private sector (which would have an operational involvement, or sometimes ownership in whole or in part) over the sector in question. One such exercise (held in November 2019) was GridEx V, which tested responses in real-time to cyber/physical threats against the North American energy grid. Over 6,500 participants from 425 government and energy sector organizations (from the, Canada, and Mexico) participated in the biennial event. Given the interdependencies and potential learning points, it is unsurprising that there was representation from other CII sectors (including telecommunications and natural gas.\textsuperscript{82}

Governments are often in receipt of the most up to date cyber threat intelligence. Mechanisms need to be devised to share information on specific threats, or provide guidance of a more general variety from time to time to the private sector. The Australian Cyber Security Centre (ACSC) for example shares detailed strategies with organizations to manage or mitigate cyber threats, with its ‘Essential Eight Maturity Model’ coming from three tiers of maturity that enables organizations to see how fully aligned they are with the mitigation strategy.\textsuperscript{83}

Public-private partnerships can be useful in several respects. Chief among them is the creation of mechanisms that enable information sharing on cyber threats. One example is the US Information Sharing and Analysis Centers (ISAC) in the US, created in 1998, as a public/private sector partnership that serves to share information on cyber threats at the industry level with the aim of protecting critical infrastructure.\textsuperscript{84} These efforts were supplemented in 2015 by the addition of more devolved (and in theory sector-agnostic) Information Sharing and Analysis Organizations (ISAO), with President Obama tellingly observing at their creation that “Government cannot do this alone. The fact is, the private sector cannot do this alone either, as the government has the latest information on threats”.\textsuperscript{85}

Other nations have developed their own models for sharing information and bringing both public and private sectors up to speed on cyber threats. The UK’s National Cyber Security Centre (NCSC) is an example. The NCSC has access to government intelligence on cyber threats, but also pools together experts from both government and private sector, disseminating its threat analyses and assessment to critical infrastructure providers in and out of government.\textsuperscript{86}

3. The Private Sector

As organizations transform their businesses, the threat surfaced has vastly enlarged, particularly with IOT devices increasingly embedded in processes.\textsuperscript{87} It has become commonplace that “there are only two types of companies – those that know they’ve been compromised, and those that don’t know. If you have anything that may be valuable to a competitor, you will be targeted, and almost certainly compromised.”\textsuperscript{88} Private sector enterprises have to consider risk mitigation and cyber resilience as seriously as the government, which itself often has limited ability or leverage to be able to enforce some of the best practices discussed above.

Certain sectors have a holistic appreciation of cyber threats, and have a strong incentive to put in place measures to protect their systems and client data. Notwithstanding several well-known successful attacks against them, financial institutions (to take one example) do regular penetration testing, and share information on threats with national cyber authorities or with the financial regulator. But in practice, this level of vigilance and mitigation is not consistently replicated throughout the private sector. One all-too-common error is treating cyber-security as an issue solely in the domain of IT specialists; another is that executives at the C-Suite level may simply treat cybersecurity as another cost item. Even where managements might be
willing to allocate resources to cybersecurity, the assumption often is that the issue can be dealt with by allocating funds in the budget cycle. Many companies fail to appreciate that this is far from sufficient. Given that cyber-threats represent in fact a global enterprise risk, mindset shifts are required from top management down, with cyber taking center stage rather than being tacked on as an afterthought.

The actual best practices for cybersecurity are well-known, and, if the right mindset exists at the management and employee level, relatively simple to implement. Some examples:

- Providing appropriate training of employees to understand the vulnerabilities (both cyber and behavioral); embedding data security in every aspect of daily operations.
- Downloading the latest security software and patches; protecting resources through regular maintenance (including remote maintenance).
- Use of two-factor authentication, or other means (for example, physical tokens) identify verification; other forms of access management.
- Use of encryption; secure connections to websites (https as opposed to http) at scale.
- Other systems safeguards (segmentation; privilege restriction; Enterprise Digital Rights Management; creating redundancies).
- Use of automated scanning and testing; endpoint detection and response.

What has been presented above should (in theory at least) operate in a situationally-aware mesh. While there are no failsafe solutions either individually or in combination, observing these tenets does afford a degree of mitigation and preparedness. Several high-profile cyberattacks have been shown through subsequent investigation to have been avoidable if such measures of a basic nature had been in place. For example, the breach of the credit reporting agency Equifax in 2017, which resulted in the compromise of data pertaining to just under 150 million individuals, could have been prevented by installing basic patches for a vulnerability that had been known for months.

One further observation: some of the most commonplace threats stem from attacks committed by “insiders.” The insider threat has been described by the DHS’ National Cybersecurity and Communications Integration Center as “…a current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization’s information or information systems.” In practice, the insider threat can extend beyond malicious employees to those who were negligent or careless (or who were co-opted in some way) in a manner that allows malicious actors to exploit, or do damage to the ICT systems and data of the company, enterprise or government agency in question. While some of the measures described further above might mitigate aspects of the insider threat, there are also other solutions that can be deployed. These include user-behavior monitoring software, or predictive analytics (incorporating tools such as machine-learning applications) that can identify behaviors that fall outside of accustomed patterns.

Corporations in the private sector as well as governments that take cyber security seriously have one thing in common – they recognize the need to develop multidisciplinary teams examining (and tasked with maintaining) cyber security from all angles – not just the technical. Experts who understand behavioral sciences are needed to complement computer and software engineers. In addition, innovative thinking should be encouraged when it comes to rooting out potential weaknesses. Bug bounty programs (where “ethical” hackers are tasked with finding weaknesses in code and applications) have been useful in both the private and public sector, and governments with a holistic view on these matters have tended to encourage a culture of ethical hacking. Separately, enterprises (as well as government agencies) sometimes employ “red cells” or “red teams” to test the level of cyber security both at the
systems and employee level. At a basic level, these teams may (just like CERTS) send out spoof phishing emails to test the levels of employee alertness. But true red teams, typically employed by agencies with a mature security posture, are capable of far more advanced activities if given the remit, and go beyond simple penetration testing. They may be allowed (for example) to try almost any measure to hack into the systems of the enterprise or agency, testing the responses of the in-house CERT.97

One final comment: the “offensive” side in cyber always seems to be one step ahead of a defense frantically playing catch-up.98 This is often not on account of technical failures such as deficiency in malware detection, but it is often tied to a lack of awareness of cyber security; indeed, many high-profile hacks have had at their root human weakness. These might span an entire spectrum, ranging from weak (and easily exploited) passwords, failure to secure Wi-Fi connections, the opening of phishing emails that contain malicious code, being lured to an online “watering hole,” or thoughtlessly inserting a compromised USB thumb-drive into an open port. It has thus become a commonplace that humans are the weakest link in cybersecurity. Several national cyber centers, including some of those mentioned above, give to the general public also guidance on cybersecurity.99 But the cyber threat is not as visible as (say) terrorism, and, unlike kinetic attacks by terrorists, the attack may have been ongoing long before the target is aware. Good cyber hygiene at the personal level is often a key component of national plans for shoring up cyber defenses. While it cannot be said that any country has achieved complete competence of cybersecurity over the government, private sector and people pillars, some have advanced further in the journey than others. The defense efforts of three countries which have gone about this are the US, Estonia, and Singapore. These will be discussed in the following case studies.

Part III: Case Studies: Estonia, Singapore, and US

“The Estonian cyberspace can be defended if the state and society as a whole participate in the defence, the necessary experts have been trained, and society is aware of the dangers of the virtual world and knows how to avoid them and acts correctly if problems occur.”

- Estonian National Security Concept, 2017100

“For Estonia, cybersecurity does not mean protecting technological solutions; it means protecting digital society and the way of life as a whole.”

- Estonian Cybersecurity Strategy, 2019-2022101

Estonia: What Doesn’t Kill You…

The internet, and the connectivity it brings, constitute the *sine qua non* to the functioning of the modern Estonian state. It is the backbone of utilities (such as the electrical grid), government communications, and services. Unsurprisingly, 99 percent of public services are dispensed online given the internet penetration was almost 90 percent in 2018.102 In 2005, Estonia became the first country in the world to hold elections over the internet, partly facilitated through the e-ID, the Estonian national digital identity system, which can be held by every Estonian (regardless of location).103 As the 2017 Estonian National Security Concept
observes, the state would be unable to function without digital services that are integrated into society – but “this increases the impact that potential attacks have on [the Nation’s] security. Due to the connectivity between communications and information systems, an interruption in one vital service may influence the availability of many others, thereby endangering the functioning of the state as a whole.”

Reaching the current level of awareness and preparedness has been a learning journey, to say the least. In April 2007, Denial-on-Service (DDoS) attacks of severe magnitude severely disrupted online services of government, media, and banking (this at a time when 97 percent of all bank transactions were conducted online, and where 60 percent of the population used the internet daily). Other targets included the Estonian Parliament. The magnitude of the attacks was such that White House cybersecurity advisor Howard Schmidt observed, “Estonia has built their future on having a high-tech government and economy, and they’ve basically been brought to their knees because of these attacks.”

Estonian officials initially pointed the finger at Russia, but subsequently, partly it appears on account of the technical difficulty in pinning down attribution, there was some backtracking. There was, however, compelling evidence of Russian links, with at least some of the hackers identifying as Russian, and with some of the attacks originating from Russian IP addresses.

The attacks were severe enough for the Estonian CERT (which had been set up in 2006) to request for international and NATO assistance. But this does not mean it was caught completely unprepared. Estonia already had a high level of technical cyber expertise, some of which had been used earlier, in 2005, to secure Estonia’s online election. This expertise, and the networks that Estonian cyber defenders (who were drawn from both the private and public sectors) had built over the years, proved useful during the 2007 attacks. International contacts were also leveraged on for assistance to block suspicious IP addresses.

Important lessons were learnt and conclusions drawn during the post-mortem, with Estonia since 2007 undergoing a complete transformation in terms of preparedness, mitigation, and response to cyberattacks. This has also encompassed a turn towards securitization of ICTs and digital technologies critical infrastructure. The latter point concerned the technical question of the architecture of ICT systems and building in redundancy. As one informed observer noted in this connection, “a distributed architecture where there is no single point of failure is way more resilient.” So seriously is “distribution” taken that some critical backup servers are now located in a data center in Luxembourg – in theory, if a cyberattack in Estonia wiped out data or if Estonian ICT and servers were to be physically destroyed or taken over through invasion or annexation, “data continuity” would be ensured and the core aspects (included land and business registries, which are among the several databases transferred) could “reboot.”

Separately, the Estonian government also subsequently decided to locate critical servers and databases in different locations throughout the country – minimizing the risk of total data failure should there be physical destruction of one site. E-health and e-ID records are for example stored in separate data centers.

**Organization**

Lessons were also learnt organizationally. In 2009, an inter-agency body, the Cyber Security Council, was established within the Security Committee of the government. The Council, chaired by the Secretary General of the Ministry of Economic Affairs and Communications, supports strategic level inter-agency cooperation and oversees the implementation of the Estonian Cybersecurity Strategy (on which more details are provided below). Also in 2009, pursuant to the first National Cyber Security Strategy issued the year before, the Department of Critical Information Infrastructure Protection (CIIP) was added to the structure of Estonian Informatics Centre (EIC), the state agency tasked with cyber security for essential information.
and communication systems. The intention was to give a strategic layer of oversight (and the
ability to give holistic recommendations) to the operational work already done by the Estonian
CERT. The EIC was itself in 2011 re-organized into the Estonian Information Systems
Authority (EISA), becoming Estonia’s central cyber security coordination center under the
Ministry of Economic Affairs and Communications. EISA is responsible for the development
and administration of state information systems, and drafting cyber policies; it has in addition
the overarching responsibility for cyber incidents Estonian networks.

Estonia has also become known as a country capable of articulating its cyber vision in a
clear-eyed manner. The first Estonian cybersecurity strategy, issued in 2008, was one of the
first of its kind in the world. The third edition, the Cybersecurity Strategy 2019–2022, expands
and amplifies on the earlier strategies. Its fundamental principles:

- Protection and promotion of fundamental rights and freedoms as important in
cyberspace as in the physical environment.
- Seeing cybersecurity as an enabler and amplifier of Estonia’s rapid digital
development, which is the basis for Estonia’s socioeconomic growth. Security must
support innovation and innovation must support security.
- Recognition of the security assurance of cryptographic solutions to be of unique
importance for Estonia as it is the foundation of the Estonian digital ecosystem.
- Transparency and public trust are considered fundamental for digital society.

Therefore, Estonia commits to adhere to the principle of open communication. The
strategic objectives of the Strategy include the following:

- A sustainable digital society: Estonia as a sustainable digital society relying on strong
technological resilience and emergency preparedness.
- Cybersecurity industry, research and development: Estonian cybersecurity industry
as a strong, innovative, research-oriented and globally competitive, covering all key
competences for Estonia.
- A leading international contributor: Estonia as a credible and capable partner in the
international arena.
- A cyber-literate society: Estonia as a cyber-literate society ensuring sufficient and
forward-looking talent supply.

The holistic approach through the emphasis on fundamental principles and strategic objectives
is especially noteworthy: what can be seen is not just recognition of the need for cyber
protection, but for awareness and cyber literacy and the building up of a capacity and talent
pipeline. Cybersecurity is not something that protects systems and CII; it is a fundamental part
of the future growth, which is why Estonia seeks to be at the forefront of the field.

People

The active involvement of the Estonian public in cyber defense is notable and has been matched
by few other nations. The Ministry of Defense, the overall authority for military aspects of
cyber defense, works closely with the Estonian Defense League, a voluntary national defense
organization. The League formed a Cyber Unit in 2010 with the aim of protecting Estonian
cyberspace and digital society (essentially, the ability of ordinary Estonians to function and
interact with each other, as well as with the government, online). Members of the unit, who
as League members are volunteers, are either IT professionals or have specific IT skills. They
are mobilized when circumstances require (for example, crisis management in the event of an
attack on CII, or boosting the capability of in-house CERTS when a specific sector comes
under attack). The unit maintains readiness through regular training and exercises, and also has a role when it comes to boosting cyber awareness in the public domain. Those involved in the Cyber Unit have, in addition to the requisite skills, a sense of duty to the country, with work in the Cyber Unit also being a useful avenue for those who for various reasons are unable to serve in the armed forces. Another attraction of the unit is that (given the nucleus of highly skilled professionals) there are good networking opportunities within, and the connections made and skills learnt in turn lead to a diffusion of competence and expertise back into the private sector.

Estonian cyber preparedness now ranks as one of the highest in the world. It has helped other nations further afield build their cyber capacity, and is also a key player in the EU’s cyber agenda. But just as important in terms of the wider multinational response that arose from the 2007 attacks is NATO’s own analysis and reaction. These are worth highlighting. Before the attacks, NATO’s focus was less on cyber threats and more on countering real-world aggression by Russia. The 2007 attacks (followed by the Russian-Georgian conflict, which took place one year after, also marked by information operations and cyber warfare) were a wake-up call – it forced an internal assessment on NATO’s cyber posture. The realization that cyber defense should now be a NATO priority in the wake of the 2007 attacks played a part in the creation of the Tallinn-based, and NATO-accredited, Cooperative Cyber Defense Center of Excellence (CCDCOE) in May 2008. The CCDCOE functions as a multidisciplinary center bringing together cyber experts, researchers, analysts from various sectors (the military, government, academia and industry) from over two dozen nations (and funded voluntarily by them). The focus is on research, development, training and education on all aspects of cyber defense. Over time, the CCDCOE has drawn in collaborations and partnerships with technology companies from the Nordic world; in addition, countries much further afield have found it useful to either maintain links with CCDCOE or plan to join it as partners.

The beginnings of the fundamental reassessment and reorganization of NATO cyber architecture can be traced to the years immediately following 2007. The year 2008 saw the formation of what was at the time NATO’s primary executive body for cyber, the Cyber Defense Management Authority (CDMA). The CDMA, headquartered in Brussels, had as its chief role the direction, coordination and assessment of the various member states’ cyber capabilities. This role, since taken over by Cyber Defense Management Board (CDMB), includes coordinating response to any cyberattack against NATO or its member states.

At the operational level, there was also fresh emphasis on the importance of the NATO Communications and Information (NCI) Agency’s NATO Computer Incident Response Capability (NCIRC TC), which has originally been set up in the aftermath of the 1999 Kosovo conflict. Following further reorganizations, centralized cyber defense for NATO came under the NATO Communications and Information Agency (NCIA), with the NCIRC becoming part of NCIA. A key part of the NCIRC was the Rapid Reaction Team (RRT), which became operational in 2012. The core of RRT is constituted of a group of experts who can be supported by further NATO professionals if the given case requires it. By the end of 2012, the RRT capability became operational.

In 2014, NATO Member States made cyber defense a core part of collective defense, declaring that a cyberattack could lead to invoking the critical NATO collective defense clause, Article 5 of the NATO Treaty. Moreover, in 2016, NATO members recognized cyberspace as a domain of military operations, (adding it to the conventional domains of air, land and sea), and further pledging to make cyber defense a priority. This was followed in 2018 by the establishment of the NATO Cyberspace Operations Centre (CyOC), which comes under the NATO military command structure. In the same year, Estonia created its own cyber command, whose mission besides cooperating with NATO allies is, inter alia, to defend the country’s information systems, and to conduct “active cyber defense” operations where appropriate.
Given the importance attached to cyber defense by the Estonian government and also given Estonia’s geographical location, it is unsurprising that some of the largest NATO cyber defense exercises are held there. An example is the NATO flagship cyber exercise (organized with the cooperation of Estonia’s Cyber Command), held in Estonia in 2019 (an earlier edition in 2016 had also been held in Estonia). Amongst the participants, besides cyber experts (including members of the Estonian Defense League cyber unit), were government officials, academic experts and individuals from the private sector.

Another major exercise is Locked Shields, organized by the NATO CCDCOE since 2010. Locked Shields is a real-time exercise that sees red team/blue teams under pressure to defend (or find a way to undermine) the cyber defenses of an unnamed country. New technological challenges are regularly injected into the exercise. The 2019 edition (which involved more than 1,200 experts from nearly 30 nations taking part) saw as the key scenario a fictional country under hostile attack, with the attacks including a cyber-component, severely disrupting (inter alia) power generation and distribution, 4G communication systems, maritime surveillance, and other critical infrastructure components. Blue teams were tasked with maintaining operations while at the same time understanding the higher strategic level calculations.

Estonia has also been an early, and innovative mover in public-private partnerships for cybersecurity and artificial intelligence (AI), with official support being given to startups in these fields. Initiatives include inviting start-ups to join its defense artificial intelligence and cybersecurity accelerator, the first of its kind in Europe. One accelerator, CyberNorth, was launched in 2019 by the business-to-business accelerator Startup Wise Guys, in collaboration with the Estonian Defence Industry Association, and supported by the Ministry of Defense. Participants benefit from intensive mentorship by industry, cybersecurity and defense sector mentors, as well as benefitting from seed money (and the possibility of further investment if successful).

Efforts are also being made to impart good cyber hygiene, and teach cyber skills, at an early stage. The Ministry of Defense (together with private sector and educational institutions) supports a program known as CyberOlympics, which aims to identify (and train) future cyber talent, and to educate the wider public (especially the young) about cybersecurity and opportunities in the cybersecurity field. One aspect is a cyber-defense competition, which sees the winners having the opportunity to represent Estonia at higher level (including international) competitions. Another aspect, CyberNuts, aimed at younger students, sees students test themselves in a survey on digital safety and cyber security, which was organized as part of the CyberOlympics project. The 2018 edition involved over 9,000 student participants.

Beneath the seemingly rosy picture of the state of Estonian cyber preparedness, it is worth noting that the 2019-2022 cyber strategy lists significant challenges, including some related to problems with strategic leadership, lack of ICT specialists, and insufficient volume of R&D. Some observers have also pointed to the fact that Estonia’s digital infrastructure suffers from a lack of investment.

The need to stay up to date has been thrown into relief through incidents in recent years involving the Estonian e-ID card. The discovery of vulnerabilities in the cards has in some cases necessitated software updates (or the revocation of security certificates). Although these do not appear to have been exploited by malicious actors, the discovery of these vulnerabilities (with the attendant potential for ID theft) does raise the issue of the security of access to government services.

Having become a model for the world, Estonia sees its cyber preparedness closely observed by other nations seeking to prepare themselves for a new generation of threats. The likelihood of its continued position as exemplar depends not just on the strides other nations make, but also on the degree to which Estonia builds on progress made since 2007 and addresses its own existing areas in need of improvement.
Singapore’s SMART Nation: “Baking” in Security

“Cyber security is a key enabler for Smart Nation. We can’t be a Smart Nation that is trusted and resilient if our systems are open and vulnerable.”

- David Koh, Chief Executive, Cyber Security Agency, 9 June 2016.143

“We have to bake [data] security into the design [of the SMART Nation].”

- Dr Vivian Balakrishnan, Minister in charge of the SMART Nation initiative, 27 November 2019.144

The Smart Nation: Opportunity and Risk

Singapore is firmly on the path to becoming a SMART Nation – a vision launched by its Prime Minister, Lee Hsien Loong in 2014.145 This is, in the words of the government agency tasked with implementing the vision,

“….an ongoing digital revolution, and advancements in digital technologies are transforming the way we live, work and play. We envision a Smart Nation that is a leading economy powered by digital innovation, and a world-class city with a Government that gives our citizens the best home possible and responds to their different and changing needs.

At the broadest level, the economy is the biggest domain driving Singapore’s growth and competitiveness. It is supported by the Government, which is leaning forward to catalyse growth and innovation across all domains, including the public sector. Crucially, these efforts are underpinned by efforts to ensure that all segments of society are able to harness digital technologies and benefit from them.”146

The nascent vision brings with it seemingly immense possibilities in terms of economic development, societal advancement, and interconnectedness (through, for example, the Internet of Things (IoT). But the vision also brings with it a vastly expanded threat surface. The SMART City generates a large amount of data which is of interest to criminal syndicates, as well as states keen to learn more about the underlying resilience and vulnerabilities of the nation.147

A second issue is awareness at the people level. Here, it is worth making a comparison with Estonia. Both countries are technologically advanced and relatively small, and both have suffered serious cyberattacks in the past. But while Estonia has a large neighbor that might attempt to undermine it from time to time, including through the use of cyber means (particularly at times when the bilateral relationship is especially fraught), Singapore has no such adversaries – at least none located at its doorstep. Singapore has, by almost all measures, been shielded for decades from major security incidents of the type that others, including near neighbors, have seen – not least terrorist attacks. This can partly be put down to an exceptionally competent security apparatus that works largely out of the limelight. But the sheer fact of Singapore’s “normalcy,” somewhat counterintuitively, weighs against efforts to protect the people and systems from cyber threats. The latter type of threats, unlike kinetic terror threats (which are visible), cannot easily be measured (since there is often no visible
damage, nor are there direct fatalities). The seemingly invisible nature of the threat therefore has bred a degree of complacency and poor security consciousness. A major nationwide cybersecurity survey conducted by the Cyber Security Agency (CSA) in 2019 found seven out of ten respondents exhibiting high levels of concerns when it came to having their computers hacked, having personal information stolen, or falling victim to an online scam. But less than half of respondents felt like they themselves would fall victim to a cyberattack.

Compounding complacency is the lack of awareness of the dangers that the much-heralded future brings. The reality of the SMART nation means innumerable IOT nodes at the individual, household or precinct level. These might include smart devices at home, personal SMART wearables, or smart CCTV systems—all might have interlinkages, and all can in theory be compromised, especially in a climate where individuals do not routinely change default passwords, and routinely log onto unsecured Wi-Fi networks.

Another concern is the security of Singapore’s Critical Information Infrastructure (CII). Singapore has eleven designated CII, which encompass sectors that are responsible for delivery of critical services. These are: government, InfoComm, energy, aviation, maritime, land transport, healthcare, banking and finance, water, security and emergency, and media. CII protection is a core part of Singapore’s Cybersecurity Strategy, launched in October 2016. One concern, falling into the category of “Digital Pearl Harbour” scenarios, has to do with the ICS and SCADA systems that play a critical role in Singapore’s utilities. The provision of some of these utilities and resources could almost be considered an existential issue—a large part of Singapore’s water supply is imported from neighboring Malaysia. Although there has to date been no major ICA/SCADA attack against Singapore’s utilities (not of the type that has caused massive disruption or physical damage), there has been a significant attack against one CII (healthcare—discussed below).

It unsurprising that CSA has in recent years organized large multi-sector cyber preparedness and crisis management exercises involving all CII operators. Separately, a masterplan developed by CSA and industry partners, the Ops-Tech Masterplan, which has a core focus safeguarding CII through public-private partnerships, has also been unveiled in 2019.

### Awareness and Talent

Singapore has decided to make cyber security a national priority. Partly in recognition of cyber threats, and also of the threats posed by hybrid activity and disinformation, a new “digital defense” pillar was added to Singapore’s Total Defense framework on 15 February 2019, the first addition of a new pillar (the others being military, civil, economic, psychological defense) since the introduction of the Total Defense concept in 1984.

Beyond the symbolic, concrete moves aimed at raising ground awareness and instilling cyber hygiene from a young age have gathered pace in recent years. CSA regularly runs campaigns targeting ordinary citizens, aimed at getting them to understand the basics (such as strong passwords, how to recognize phishing emails). CSA’s Cybersecurity Awareness Campaign began in 2017 and, into its third edition in 2019, involves roadshows for the general public, including in educational institutions. There is the recognition, like in Estonia, that the youth are a demographic segment that should be particularly drawn in early into the cybersecurity ecosystem. Besides working cooperation with the Ministry of Education to introduce cyber wellness programme in schools, CSA runs Singapore Cyber Youth Programme (SG Cyber Youth), which has multiple sub-initiatives within it. An example is the Youth Cyber Exploration Programme (YCEP) boot camp, which saw in 2019 all five polytechnics in Singapore hosting 400 students from over 30 secondary schools. The top students from these boot camps took part in the inaugural YCEP Central Capture-the-flag (CTF) Competition. CSA also plans to reach out to thousands of youths in the coming years through boot camps, competitions, learning journeys and career mentoring sessions.
Bug bounty programs have also been used with increasing regularity by government agencies. A major such program is run by GovTech, which has the lead role in implementing Smart Nation vision and leading the government’s own digital transformation. These programs thus far appear to have proved reasonably effective in unearthing vulnerabilities; added plusses include demonstrating a culture of openness and willingness on the part of officialdom to engage with the ethical hacking community, in addition to spotting talent that can potentially contribute to national cyber defense down the line in more tangible ways.

**Government/Government-linked Systems**

Singapore consistently ranks highly in various regional and international surveys of cyber preparedness and readiness. But these have not prevented Singapore, its government agencies, and other institutions within the country from being the victim of cyberattacks, with David Koh, Chief Executive of the Cyber Security Agency of Singapore, observing “Singapore is under constant attack on the cyber front. We are a prime target for cyber criminals, gangs, hacktivists and even state actors.”

Some of the best-known cyberattacks have targeted government agencies. The IT system of the Ministry of Foreign Affairs (MFA) was breached in 2014. In another cyberattack in 2017 against a Ministry of Defense system providing system internet to personnel working in Singapore Armed Forces (SAF) premises, hackers stole national identity card numbers, telephone numbers and birth dates of approximately 850 personnel. Other noteworthy cyberattacks that did not directly target government ministries, but targeted data linked to government. In April 2017, in the first sophisticated cyberattack against Singapore universities, hackers infiltrated the networks of the National University of Singapore (NUS) and the Nanyang Technological University (NTU) in what appeared to have been an attempt to steal sensitive government and research data.

Internet separation was implemented on government networks in 2017, affecting approximately 143,000 civil servants. It was recognized, even at the time of implementation, that the measure was not a fool proof solution to protect government servers. But the aim was to afford some mitigation - to prevent malware finding its way into classified government systems, and to prevent classified emails from finding their way to unsecured computers and personal devices.

**The SingHealth/IHiS Breach**

Internet separation has something of a bearing on Singapore’s worst cyberattack in its history, which took place between June and July 2018, targeting Singapore’s health records system. The agency targeted, Integrated Health Information Systems (IHiS), was the central IT agency responsible for Singapore’s healthcare sector. IHiS was not a government ministry, but the data compromised (1.5 million SingHealth patients and the outpatient prescription records of 160,000 others, with the health data of Singapore’s Prime Minister repeatedly targeted) came under SingHealth, Singapore’s largest cluster of public healthcare institutions. The attacker was well-resourced and persistent, with the authorities suggesting that an unnamed state actor lay behind the APT responsible for the breach. Malicious activity finally came to a complete halt after internet surfing separation was implemented on SingHealth systems on 20 July 2018.

The high-level Committee of Inquiry (COI) examining the causes of the breach as well as the response to it found lapses in procedures and especially human weaknesses. While some individuals in the incident response team had attempted in the midst of the attack to remediate
matters, there were also basic failures (on the part of a key incident response manager) when it came to recognizing the severity of the attack, and (somewhat startlingly) recognizing what in the first place constituted a security incident. These human failures, besides leading to delays in the ongoing attack being reported up the chain of command and to authorities such as CSA, also meant that opportunities to mitigate the effect of the cyberattack were missed.\textsuperscript{169}

The inquiry made 16 main recommendations to improve processes and prevent a recurrence. One category of priority recommendations concerned improving competencies and staff awareness (including more effective incident response), as well as levels of cyber hygiene. The recommendations also included ensuring privileged administrator accounts would be subject to greater monitoring, and the use of two-factor authentication when engaged in administrative tasks. On the “technical” side, recommendations included real-time monitoring of databases, implementing a robust patch management to address security vulnerabilities, and putting into place controls to better protect against data theft.\textsuperscript{170}

Beyond policy-related and technical aspects of the recommendations, more important was the overall philosophy the COI took, as these had implications for cyber preparedness in all other large organizations that might have data others covet. The COI in its report suggested the near-inevitability of sophisticated attackers being able to breach any network. Organizations therefore had to adopt an “assume breach” mindset and “defence in depth” strategy. This involves inter alia: arming themselves with sophisticated security systems and solutions which can facilitate early detection of malware, and by adopting emerging technologies, such as database activity monitoring endpoint detection and advanced behavior-based analytics.\textsuperscript{171}

Breaches like the IHiS/SingHealth incident have the potential to affect public confidence in the government as custodian of public data.\textsuperscript{172} As a result, the government in March 2019 convened a high-level Public Sector Data Security Review Committee, chaired by the minister in charge of Public Sector Data Governance. The five main recommendations of the Committee (which reviewed data management practices across all 94 public agencies to identify risk areas) will be mentioned here as they have a bearing on cyber preparedness:

- Improving data protection and preventing data compromise through measures like protecting data directly when stored to ensure it is unusable even if extracted.
- Improving detection and response to data incidents through measures like designating the Government Data Office to monitor and analyze data incidents that pose significant harm.
- Raising competencies and instilling a culture of excellence through measures such as training all public officers to attend improved data security training every year.
- Accounting for data protection at every level through measures like amending Singapore’s Personal Data Protection Act to cover third-party vendors handling Government data.
- Ensuring a continuous approach to improving data security through measures like improving the Government’s expertise in data security technology.

Lapses found by the committee (members of which were present in the majority of agencies reviewed) included failings in management of privileged user accounts, user access reviews, and encryption of emails with sensitive data.\textsuperscript{173} These findings came on top of earlier government audit findings made public which had similarly pointed to weaknesses in government agencies’ IT controls.\textsuperscript{174}

A concerted push to accelerate remediation could be discerned from late 2019 onwards, with the Smart Nation and Digital Government Group (SNDGG – which consists of the Smart Nation Office under the Prime Minister’s Office and GovTech), working with public agencies to effect deep changes at the “technical, process and people levels to address the systemic causes” behind findings of vulnerabilities by earlier committees. Announced in early January 2020 were several measures to reduce vulnerability at the IT, systems, and people level. These
pertained to areas of concern that had been flagged repeatedly by previous committees, such as the introduction of automated tools across government agencies that would enable review of the activity logs of privileged user accounts and flag any unexpected behavior, with a new system planned that would perform targeted checks using audit and incident data. Finally, in the works is a comprehensive revision of the government instruction manual dealing with IT security, with the new standards to be benchmarked against leading industry practices.175

These initiatives to protect government systems and data require adequate funding. February 2020 saw the announcement during the course of the annual Parliamentary budget debate of $1 billion over the next three years to build up the Government’s cyber and data security capabilities. The funds will be used to safeguard citizens; data and critical information infrastructure systems, with the Deputy Prime Minister and Finance Minister Heng Swee Keat emphasizing in the course of his announcement how data security is a vital prerequisite and key enabler of Singapore’s digital economy.176

The Private Sector

One of the SingHealth/IHiS COI recommendations was that partnerships be formed between government and industry to achieve a higher level of collective security.177 There have been some positive developments. A case in point is the launch of a joint venture center of excellence (a partnership between an entity partly-owned by a government investment arm and IronNet, founded by former NSA Director Gen (retd.) Keith Alexander) to protect critical infrastructure against sophisticated cyberattacks.178

However, at the level of ordinary business, significant issues exist. Some of these have to do with factors cited further above which are common to companies around the world: key personnel at the management or C-suite level might still view cybersecurity as purely a IT issue (not a business risk), with investments in cybersecurity seen as a cost item on the balance sheet.179 While major multinationals and institutions such as banks may have the resources and the perspective to recognize the need not just for investments in cybersecurity but also for the right mindset, a lack of knowledge and resources is preventing local small and medium enterprises (SMEs) from adopting robust cybersecurity measures.” Many attacks that target SMEs come either from pre-identified risks or from insider threats.180 CSA and other agencies such as the Infocomm and Media Development Authority (IMDA) have worked on this issue. On offer are tailored cybersecurity solutions and a one-stop portal to access grants to acquire and deploy these solutions.181

Observers of Singapore’s SMART Nation drive will have been given considerable food for thought by events of recent years. Despite many positives, it is clear that all major constituents - government, private sector, and citizens and residents – still have areas for improvement. The private sector needs (especially below the level of MNCs and other well-resourced entities) to take cybersecurity more seriously and to see it as a continuing enterprise risk. The government needs to heed lessons of various lapses and breaches; lest the overall levels of public confidence reposed in the state to keep Singapore safe start to dip (of which there has been no sign yet). The people, for their part, can only progress to a certain level of maturity if the key drivers of awareness and education remain the slew of well-intended initiatives from relevant government agencies. If the people themselves are not seized with these issues, there may be further amplification of the sentiment, evinced already by some observers, that the weakest link in Singapore’s cybersecurity efforts may well be the people.182

All this will in turn have a bearing on Singapore’s future. It will certainly, given time, become a truly SMART Nation. But will it become a secure SMART Nation?
United States of America

The US was a pioneer in national approaches to securing cyberspace, with the national security and intelligence communities aware since the 1990s that various state and non-state actors could seek to undermine or cause outright damage to the country through cyber means.\textsuperscript{183} This has been a continuing – and developing – threat perception. The 2019 Worldwide Threat Assessment given by Director of National Intelligence (DNI), Dan Coats, before the Senate Select Committee on Intelligence ranked cyber as the number one threat, above terrorism.\textsuperscript{184} Every DNI Worldwide Threat Assessment (which represents the consolidated view of US intelligence agencies) from 2013 onwards had presented cyber threats above terrorism in its hierarchy of threats to the US. Securing cyber national space poses enormous challenges to the many agencies concerned. The enormous attack surface includes the government at the federal and state levels, as well as the private sector, together with CII (mostly under the control of the private sector). Some of this is relatively well-defended, but in many cases, resources, manpower and expertise are lacking. Compounding the issue are interagency rivalries, and differing perspectives and threat perceptions between private sector and the federal government.

The sense of heightened vulnerability in the years immediately following the 9/11 attacks included something of a fixation with the possibility Islamist terrorists might acquire cyber capabilities.\textsuperscript{185} This proved to be temporary, with Richard Clarke, the first White House Adviser for Cybersecurity, stating in 2002 that “there are terrorist groups that are interested in conducting cyberattacks. We now know that Al-Qaeda was interested. But the real major threat is from the information-warfare brigade or squadron of five or six countries.”\textsuperscript{186} Some of the major US initiatives after 9/11 are worth remarking on here.

- The Office of Homeland Security (which was later in 2002 to become the Department of Homeland Security (DHS)) was given overall authority for the protection of critical infrastructure against threats (but not, as we shall see, made the overarching body responsible for cyber issues). In 2003, the National Cyber Security Division was created within the DHS, with the first US CERT coming under this division.\textsuperscript{187}
- The establishing by Executive Order of the President’s Critical Infrastructure Protection Board (CIPB) and the appointment of Richard Clarke, from the National Security Council, and former national coordinator for security, infrastructure protection and counterterrorism, as the first White House Special Adviser for Cyber Security and chair of the CIPB.\textsuperscript{188}
- The CIPB published under Clarke’s leadership the National Strategy to Secure Cyberspace in February 2003. This, the first such official strategy, was a foundational document, identifying eight major planks for effective cyber preparedness and response:
  1. Establishing a public-private architecture for responding to national-level cyber incidents;
  2. Providing for the development of tactical and strategic analysis of cyberattacks and vulnerability assessments;
  3. Encouraging the development of a private sector capability to share a synoptic view of the health of cyberspace;
  4. Expanding the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security;
  5. Improving national incident management;
  6. Coordinating processes for voluntary participation in the development of national public-private continuity and contingency plans;
  7. Exercising cybersecurity continuity plans for federal systems; and
8. Improving and enhancing public-private information sharing involving cyberattacks, threats, and vulnerabilities.189

Early exercises and penetration testing in the late 1990s and early 2000s did not give ground for a great deal of optimism when it came to the state of overall US preparedness. A well-known example is the 1997 exercise, code-named “Eligible Receiver” conducted by the National Security Agency (NSA). NSA hackers acting as a “red team” posing as North Korean hackers, penetrated various national security systems, including Pentagon computer systems (and in several cases, doing so with some ease, using brute force hacking, social engineering, and also through using off the shelf hacking tools that were relatively easily obtainable).190 The results were alarming to the national security establishment, to say the least. The impression that the government was ill-prepared to defend itself against burgeoning cyber-threats was reinforced by several further exercises and studies in the years immediately following. Two cases in point: a 2003 study by the House Government Reform Subcommittee on Technology, which examined (and graded) cyber security in various federal agencies, awarded more than half the federal agencies surveyed a low or failing grade (D or F), including the DHS.191 In 2006, Exercise Cyber Storm (itself overseen by the DHS), designed to test reactions of government agencies and the private sector to cyberattacks against key CII, found that participants across both government and the private sector had difficulty responding effectively to attacks (and indeed, in some cases, recognizing the attacks in the first place).192

The Obama Era

Particularly since the beginning of the Obama era, there was a move to enhance the sense of cybersecurity responsibility within the private sector, with, as one commentator observes, the White House “focused on helping the private sector protect itself, instead rather than trying to make cybersecurity a government responsibility.”193 This was understandable: private industry owns and operates about 85 percent to 95 percent of the US critical infrastructures, and, in theory at least, has the resources and expertise for ensuring the security of these assets. The posture taken by relevant government agencies was to provide support in appropriate areas (for example, in law enforcement aspects and investigations, and, where appropriate, information sharing).194

The difficulty is that many companies prefer not to have an overly-close relationship with government agencies when it comes to cybersecurity. The better-resourced companies may have in-house CERTs, while others may prefer to use specialist providers (which may be able to respond more quickly than the government). Many private sector companies, once they have recovered from a breach, may be reluctant to work closely with government agencies when it comes to post-breach forensics, as (from their point of view) this might be exposing themselves to added scrutiny. Other weaknesses and vulnerabilities might be exposed, with government agencies possibly demanding additional mitigating measures for these while not seeming to have that much to offer in return.

Finally, the private sector is not necessarily hardwired to see the national security implications of a major breach. A case in point is the November 2014 hacking of Sony Pictures by a group calling itself the “Guardians of Peace.” The attack was believed to be taken in response to The Interview, a middling Hollywood movie depicting the assassination of North Korean leader Kim Jong-un. Besides rendering many workstations inoperable, large amounts of data and emails were stolen, with some released to the public in a way that caused severe embarrassment to Sony.195

Weaknesses within Sony were partly to blame for the hack. Cybersecurity practices were extremely careless at best, and at worst, institutionally negligent. There was awareness at the management level of Sony’s parent company of various failings, with internal IT assessments...
before the cyberattack showing that basic security protocols were ignored. The internal network had hundreds of unmonitored devices; in addition, passwords for Sony Pictures’ internal computers were stored without even basic protection.196

The FBI moved quickly, attributing the hack to North Korea within weeks.197 But it appears that outside of government, and particularly within the entertainment industry, many were skeptical on the attribution. In these circles, there also appeared to be an unwillingness to accept the potential seriousness of the incident.198 The Sony hack convinced influential figures within the administration that the US had to impose penalties for cyber misbehavior.199

The Sony hack was something of a turning point: senior figures within government realized that the private sector when faced by a cyber-threat of serious magnitude would not be able to deal with the threat on its own; nor would it be able to appreciate the wider implications of a state-linked attack. Both the public and private sectors have to be prepared to cooperate when it comes to incident response.200 National Security Agency Director Michael Rogers called the attack a game-changer, and “a national-security issue that crosses almost every spectrum of our society.” Emphasizing that government and private sector had to find ways work together to deter and respond to cyberattacks, Rogers also observed that there had to be clarity when it came to giving the private sector a sense of what they could expect from the authorities, and what they had to do, in the event of a major breach.201

Despite these initiatives, the legacy of the Obama presidency when it comes to the overall shoring up of the nation’s cyber defenses was rather mixed. To be sure, there was a substantial amount of intellectual heavy lifting, as evidenced by the 2009 Cyberspace Policy Review, which aimed at producing a “coordinated cybersecurity plan” intended to, amongst other points, build capacity and pave the way to create effective information sharing mechanisms in the event of cyberattacks. The resulting cybersecurity strategy also meant, theoretically, something of centralization of cybersecurity efforts that saw an overarching cybersecurity coordinator appointed within the White House.202

There were other achievements. In 2013, the National Institute of Standards and Technology was directed by executive order to work with the private sector to develop the Cybersecurity Framework, a common set of (voluntary) cybersecurity best practices. This was finalized in December 2014.203 The following year, President Obama signed the Cyber Information Sharing Act (CISA) designed to improve the sharing of threat information between federal government and the private sector.

CISA was a step in the right direction, but it did not represent a comprehensive (nor binding) instrument to get the private sector to work with the government. Notwithstanding the administration having a vision in terms of where the government and private sector had to go in improving cyber security, observers were by the end of the Obama presidency questioning how much all the measures enacted had actually improved the nation’s overall state of cyber readiness. Criticisms included the government’s use of outdated technology, as well as the failure to keep pace with the evolving nature of cyber threats.204

**Inter/Intra-Agency Dynamics**

On top of these criticisms was the issue of interagency turf squabbles. Which agency actually took overall responsibility for cybersecurity? CISA technically meant that DHS had become the node through which the private sector could share threat information (rather than companies going directly to agencies such as the FBI or NSA).205 CISA built also on the National Cybersecurity Protection Act of 2014, which had officially authorized and codified the role of the DHS’ cybersecurity information sharing hub, the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC would provide a platform for the government and private sector to share information about cybersecurity threats, incident response, and technical assistance. But CISA did not explicitly make DHS the lead cyber
agency; other well-resourced agencies such as the NSA and the Pentagon all had major stakes and chafed at the notion that they should be subordinate to the DHS on cyber matters. They also did not believe that DHS could adequately protect the nation from cyber threats.\textsuperscript{206}

More clarity was, relatively speaking, reached in 2018 with the passing of the Cybersecurity and Infrastructure Security Agency Act (CISA; not to be confused with the Cyber Information Sharing Act above).\textsuperscript{207} CISA was created out of the former National Protection and Programs Directorate (NPPD) within DHS. Its core responsibilities included protecting the nation’s critical infrastructure from physical and cyber threats, safeguarding government systems, providing cybersecurity governance, and working to build the national capacity to defend against and cyberattacks.\textsuperscript{208}

Two other DHS-related developments that show its growing maturity are worth remarking on here. The first concerns the 2017 revamp of CISA’s National Cybersecurity and Communications Integration Center (NCCIC), which is the DHS’s node for cyber that sees to it that operational elements are coordinated and integrated. NCCIC provides daily operational cyber awareness, analysis, incident response and cyber defense capabilities to both the US federal government and to local authorities (as well as the private sector). The reorganization saw functions previously performed independently by the US Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) integrated into the NCCIC.\textsuperscript{209} The second development was the release in 2017 of the DHS’ National Cyber Incident Response Plan (NCIRP), an important doctrinal document that delineates various lines of effort and clarified roles and responsibilities (for of the Federal Government, the private sector, and SLTT (State, Local, Tribal, and Territorial) government) in the aftermath of cyber incidents, showing also how the DHS would manage the effects of significant cyber incidents.\textsuperscript{210}

CISA collaborates regularly with partners when it comes to instilling a culture of cyber preparedness nationwide. The Federal Emergency Management Agency (FEMA) facilitates its National Level Exercise (NLE) every two years, with the 2020 NLE event focusing on cybersecurity. NLE 2020, which draws participants from government as well as the private sector, will integrate CISA’s cyber exercise CyberStorm (which is itself biennial).\textsuperscript{211} In addition to the NLE, FEMA (again in partnership with CISA) regularly runs smaller table top exercises and roundtables, bringing together participants from federal, state and local agencies (and also including representatives from academia and the private sector) to test and run through response plans to cyber threats.\textsuperscript{212}

Another key player in the interagency mix is the Department of Defense (DoD) Cyber Command (USCYBERCOM). Achieving fully operational status in 2010, USCYBERCOM Command was in 2017 elevated to the status of a Unified Combatant Command focusing on the planning and execution of cyberspace operations against adversaries of the US (another key role is ensuring the security of DoD networks). USCYBERCOM has in recent years refined the way it measures success. It now seeks to enable other government agencies, as well as industry, to defend against cyber threats.\textsuperscript{213} In doing so, USCYBERCOM collaborates (and shares information with) with partners such as CISA and the FBI.\textsuperscript{214}

**Threats and Threat Actors**

The vulnerability of critical infrastructure to cyberattacks has been recognized for a quarter of a century. July 1996 saw the formation of the President’s Commission on Critical Infrastructure Protection (PCCIP) to study vulnerabilities of critical infrastructures and propose protection strategies.\textsuperscript{215} In its final (and influential) report, issued in October 1997, the commission noted that the interdependences of various critical infrastructures were real and that, through mutual dependence and interconnectedness, attacks on vulnerabilities “could have severe consequences for our economy, security, and way of life.”\textsuperscript{216}
The rise of ISIS revived the question whether this jihadist organization could surpass Al-Qaeda and achieve a level of sophistication and capability to carry out destructive cyberattacks against American CII. In May 2015, FBI Director James Comey observed that ISIL was “waking up” to the idea of using sophisticated malware to cyberattack critical infrastructure in the US. But, although senior officials were at around this time observing that ISIS seemed to be attempting to target critical infrastructure, there was very little by way of hard evidence, and none concerning major attacks. While ISIL appears to have the intent, attempted attacks do not seem to have risen further than DDOS, defacement, and other, relatively minor, breaches.°

The real threat remains the same: state actors which have the technological capability and intent, with means to cause damage of a serious magnitude growing in parallel with the increasing sophistication and interdependence of CII. In 2012, General Keith Alexander, National Security Agency director and commander of the US Cyber Command, stated that cyberattacks against US information networks started as exploitative before becoming disruptive, but now such attacks are moving into the realm of destructive. Gen. Alexander’s successor in both these positions, Admiral Mike Rogers suggested in 2014 that:

“… the threat of a catastrophic and damaging cyberattack in the United States critical infrastructure like our power or financial networks is actually becoming less hypothetical every day.... Foreign cyberactors are probing Americans’ critical infrastructure networks and in some cases have gained access to those control systems. Trojan horse malware that has been attributed to Russia has been detected on industrial control software for a wider range of American critical infrastructure systems throughout the country. This malware can be used to shut down vital infrastructure like oil and gas pipelines, power transmission grids and water distribution and filtration systems.”

Elsewhere, Admiral Rogers also pinpointed the key state actors – Russia and China – which posed the most serious cyber threats to the US, stating that they “count as peer or near-peer competitors in cyberspace.” It is, for example, Russia that has carried out reconnaissance against the US energy grid. DHS threat warnings to critical infrastructure operators have precisely highlighted this threat, providing details on how cyber actors linked to the Russian state targeted networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government’s cyber actors conducted network reconnaissance and collected information pertaining to Industrial Control Systems (ICS). Besides the energy sector, other targets have included nuclear, aviation, critical manufacturing and the water sector.

Iran and North Korea were the other threat attacks singled out by Admiral Rogers. Despite having fewer technical tools, Rogers noted that they “employ aggressive methods to carry out malicious cyberspace activities,” with Iran recruiting hackers for cyberespionage and cyberattacks, including attempts to penetrate US military systems. Iran appears to have ratcheted up attempts at cyberattacks against US targets following the assassination in January 2020 of Qassem Soleimani, the head of the Iranian Revolutionary Guard Corps’ Quds Force. Yet, attempted cyberattacks by Iran or its proxies have in fact already been ongoing for some time – and not simply against military targets. Between 2011 and 2013, Iranian hackers (linked by the US to the Islamic Revolutionary Guard) carried out a series of attacks on the largest US financial institutions including J.P. Morgan Chase, Wells Fargo, Bank of America, and Citigroup. These hackers for the most part employed relatively unsophisticated DDoS attacks in 2013.

It is not just the major players within CII that are vulnerable. Smaller, often regional, players often invest less resources in cybersecurity, assuming that they are somehow below the radar and immune from the threat. But one or more individuals from the Iranian group above...
attempted to penetrate the SCADA system of the Bowman dam in Rye, New York, in August and September of 2013. Although the dam was small, the access obtained would have permitted the hacker to remotely operate the dam’s sluice gate, if it had not been for the fact that the gate had been disconnected for maintenance at that particular time. Another case in point is the attacks in 2019 against small electricity providers (many in proximity to critical infrastructure) in 18 different states. These attacks (which attempted to use phishing techniques to implant malware) do not appear to have succeeded, and may have been more akin to preliminary reconnaissance operations than genuine attempts to cause serious disruption. Separately, in December 2015, a group of hackers managed to infiltrate a water treatment plant (the exact location of which has not been made public) and change the levels of chemicals being used to treat tap water. The breach happened as the water company had been using operating systems which were more than a decade old to run its entire IT network. This server is also connected to the operational technology (OT) systems of the facility. Serious damage appears to have been averted as the hackers did not have detailed knowledge of the ICS/SCADA system.

China’s cyberattacks against US targets include espionage (both industrial theft and the theft of military or sensitive government data), with officials not ruling out the possibility that, like Russia, China might be attempting preposition cyberattacks against critical infrastructure. Attacks against utilities have also been attributed to hackers working on behalf of the Chinese state.

Some cyberattacks attributed to China stand out in particular. The 2017 Equifax hack has already been discussed. Besides this, perhaps the best-known of all publicly-reported cyberattacks in the US attributed to China is the US Office of Personnel Management (OPM) hack. In 2013, hackers linked to China breached OPM networks, leading to an unprecedented leak of sensitive data of personnel (with personnel records and security-clearance files of approximately 22.1 million individuals, including federal employees and contractors compromised). What came to light after the breach were revelations of internal neglect, and extremely poor IT security within OPM and its contractors. Earlier reports had flagged significant and “persistent deficiencies in OPM’s information system security program,” but there was a great deal of lethargy when it came to taking remedial action. Basic failings included the lack of multi-factor authentication for users remotely accessing OPM systems.

The US government’s CERT in CISA periodically issues warnings, and advice, on the persistent cyber threat emanating from certain quarters. US CERT has observed that Chinese threat hackers are exploiting relationships between managed IT service providers and their customers. This space is a tempting target given that IT services have access to their customers’ networks. Some of the suggestions aimed at protecting against Chinese threat actors are not altogether too different from recommendations issued in other countries. US CERT is encouraging clients to implement a defense-in-depth strategy to protect their infrastructure assets and increase the probability of successfully disrupting APT activity. This is similar to (and pre-dates) the recommendations issued by the Committee of Inquiry in Singapore examining the IHIS breach. Measures recommended by US CERT include:

- Applying the principle of least privilege to their environment, which means customer data sets are separated logically, and access to client networks is not shared.
- Implementing robust network and host-based monitoring solutions that looks for known malicious activity and anomalous behavior on the infrastructure and systems providing client services.
- Ensuring that log information is aggregated and correlated to enable maximum detection capabilities, with a focus on monitoring for account misuse; and
- Working with customers to ensure hosted infrastructure is monitored and maintained, either by the service provider or the client.
Talent Acquisition and Future Challenges

Finding the right cyber talent is a pressing issue in every nation, but especially problematic in a nation like the US that spreads cyber responsibilities across a multiplicity of agencies, and where both state and federal levels are competing with the lure of the private sector. In August 2017, the then-White House cybersecurity coordinator Rob Joyce warned that the US lacks 300,000 cyber-security experts needed to defend the country.\(^{233}\) One comprehensive report in 2018 by Harvard’s Kennedy School and Belfer Center has pointed to the “shortage in skilled cybersecurity-minded talent” at the federal level.\(^{234}\) CISA Director Chris Krebs has himself weighed in, noting that talented cyber professionals would rather choose careers in big tech companies.\(^{235}\) Efforts are underway to remediate, with the Cybersecurity Talent Management System announced in 2018 allowing the DHS to speed up hiring and offer higher salaries for cyber professionals. At least in theory, this should enable the federal government to compete with the private sector for cyber talent. One other facet of this plan involves the government paying for scholarships for cybersecurity professionals, who, under the plan, will have to spend three to five years in government before moving into the private sector. Originally slated for implementation in 2019, the Talent Management System has at the time of writing (February 2020) not yet been officially implemented.\(^{236}\)

The American National Guard has in various states begun to develop cyber units. Some have already shown their value in remediating the effects of state-level ransomware attacks.\(^{237}\) Separately, cyber personnel from the National Guard make up Task Force Echo (which currently has a strength of approximately 450 personnel drawn from the Army National Guard), which supports USCYBERCOM’s mission.\(^{238}\)

Task Force Echo, while filling a critical role for USCYBERCOM, has, however, been criticized as “lacking societal engagement and offering no way of integrating private-sector talent.”\(^{239}\) The US has long recognized the need for volunteers to help fill the gaps in its cyber defense efforts. Other, more innovative solutions to fill the talent vacuum have from time to time been floated. Some have suggested that the US needs its own cyber volunteers, akin to the Cyber Unit within the Estonian Defense League.\(^{240}\) There are in fact already in existence a few examples of looser groupings, akin to cyber militia, coming together in the US in order to provide assistance in the wake of cyber incidents (and particularly in the event when federal assistance might not be immediately forthcoming). The Michigan Cyber Civilian Corps (MiC3) established in 2013, comprises approximately 100 volunteers from government, academia, and business and serves as a rapid response force against cyber incidents within Michigan.\(^{241}\) Some commentators have suggested that it is imperative that this type of effort be scaled up into a US Cybersecurity Civilian Corps.\(^{242}\)

Beyond simply protecting networks on a routine basis, it is likely that Task Force Echo and MiC3 will increasingly have roles assisting frontline agencies such as CISA in protecting critical processes such as elections. As has been well-documented, Russian hackers were extremely active in the run-up to the 2016 U.S. presidential election. Besides the manipulation of societal opinion through social-media-enabled subversion (via bots, troll factories), Russian hackers also broke into the Democratic National Committee’s email servers. Russian hackers also attempt to seek out vulnerabilities in state election infrastructure. In certain states’ voter databases, Russian hackers were in a position to delete or change voter data (although it appears they refrained from doing so).\(^{243}\)

Interference in the democratic polity and the electoral process are best known from the Russia case study, but others have made attempts of their own too. In late 2019, a hacking group that appears linked to the Iranian government tried to infiltrate email accounts related to Trump’s re-election campaign.\(^{244}\) Suffice to say that the inference in 2016 will not be a one-off. Chris Krebs, Director of CISA (the federal agency with primary responsibility for assisting state and local officials in bolstering election security), observed in February 2020 that he spent “40 to 50 percent of my time on election security issues (…) A top priority for us right now is
Besides election security, CISA’s other operational priorities, outlined in its “strategic intent” plan from 2019, include defending against Chinese threats to 5G networks and reducing the risk of Chinese supply chain compromise.

Protecting against a new generation of cyber and technology-enabled threats will be a critical concern for CISA, USCYBERCOM, and various state and local agencies in the years to come. In this battle against adversaries – many located thousands of miles away - metrics of success are vague and the successes themselves are often hidden under a cloak of operational secrecy. Achieving a better cybersecurity posture will lie not simply in technological prowess, but in strengthening a culture of awareness and responsibility, enhancing interagency cooperation, and in nurturing an ecosystem where cyber talent can flourish and can be directed to where it is needed the most.

Dr. Jayakumar is Head, Centre of Excellence for National Security (CENS) and Executive Coordinator, Future Issues and Technology at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. Shashi Jayakumar was a member of the Singapore Administrative Service from 2002-2017. During this time, he was posted to various ministries, including the Ministries of Defence, Manpower, Information and the Arts, and Community Development, Youth and Sports. From August 2011-July 2014 he was a Senior Visiting Research Fellow at the Lee Kuan Yew School of Public Policy. His research interests include extremism, social resilience, cyber issues, and homeland defense.

Acknowledgments

The author would like to acknowledge the assistance of Beatrice Lee and Benjamin Low in the preparation of this article. All errors and omissions remain the author’s own.
Endnotes

3 Denning, D. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, Committee on Armed Services, 23 May 2000. Available at: https://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf
7 For observations on the advantages that social media platforms and networking sites give terrorist groups, over and above online fora and websites, see Gabriel Weimann, ‘Terrorist Migration to Social Media’ Georgetown Journal of International Affairs, Vol. 16, No. 1 (Winter/Spring 2015), pp.181-183.
12 Cf Catherine Herridge, Catherine ‘Al Qaeda video calling for cyberattacks on Western targets raises alarm in Congress’ Fox News, 22 May 2012. Available at: https://www.foxnews.com/politics/al-qaeda-video-calling-for-cyberattacks-on-western-targets-raises-alarm-in-congress
19 Alexander, Audrey and Bennett Clifford, ‘Doxing and Defacements: Examining the Islamic State’s Hacking Capabilities’, CTC Sentinel, April 2019, p. 25. Available at: https://ctc.usma.edu/doxing-defacements-examining-islamic-states-hacking-capabilities/.
20 Ibid. For other examples of releases of large Kill lists by ISIS-linked groups, see ‘Pro-ISIS Hacking Group Releases Kill List Targeting Canadians, Containing Over 12,000 Entries’, MEMRI Cyber & Jihad Lab, 29 June 2016. Available at: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-hacking-group-releases-kill-list-targeting-canadians-containing-over-12000-entries/.
22 Murphy 2015; Lamothe 2015.
23 It is important to note that many of these pro-ISIS collectives, including the UCC and the Cyber Caliphate Army, never appear to have had a formal association with ISIS “Central”. The history, nomenclature and evolutions of the cyber/hacking groups said to be part of, or linked to ISIS’s central arm is by no means straightforward. Many with grand names may be devolved individuals, having no formal link with the terror organization; further complicating the picture is that the recent history of groups claiming some sort of affiliation with ISIS is littered with unproven claims of mergers and associations of groups which have gone by various names, including the Caliphate Cyber-Army, Sons Caliphate Army and Kalashnikov Team, and the United Cyber Caliphate (said, in some accounts, to be the organization formed by fusing the aforementioned disparate groups). For a discussion, see Rose Bernard, ‘These are not the terrorist groups you’re looking for: an assessment of the cyber capabilities of Islamic State’, Journal of Cyber Policy, Vol. 2, No. 2,2017, pp. 258-260. See also the comments of Laith Alkhoury, Alex Kassirer and Allison Nixon, in ‘Hacking for ISIS: the Emergent Cyber Threat Landscape’, Flashpoint, April 2016, p.19.
24 Wolf, K., ‘Cyber Jihadists Dabble in DDoS: Assessing the Threat’, Flashpoint, 13 July 2017. Available at: https://www.flashpoint-intel.com/blog/cyber-jihadists-ddos/. For a detailed study of the UCC (which appears to have coalesced in 2016 as the result of the merger of previously distinct groups) and its capabilities, see Nadine Liv, United Cyber Caliphate, International Institute for Counter-Terrorism, 20/3/2019. Available at:
The UCC in some of its cyber operations also appears to have managed to compile “kill lists” by accessing servers that held data of Saudi soldiers. In yet another operation, the UCC released on its Telegram channel another kill list containing over 8,000 names and identifiers, mainly from the US and UK. Nadine Liv, *United Cyber Caliphate*, pp. 12-13; Chris Summers, ‘ISIS orders American lone wolf jihadis to slaughter 8,000 citizens by releasing ‘kill list’ which includes the names of several Hollywood celebs’, *The Daily Mail Online*, 9 June 2016.


There is some evidence that Hamas has a hacking wing. This came to light in May 2019, when the Israeli Defence Forces (IDF) announced the destruction of a building in Gaza where Hamas hackers were located. Details were scant on what the target of the Hamas cyber activity was (it appears to have been stopped online) and how advanced this capability was, but clearly it was of a nature that necessitated an immediate, real-world retaliation. The Israeli response was noteworthy as it may mark one of the first occasions that a kinetic action was made in response to hacking activity. Kate O’Flaherty, ‘Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A World First’, *Forbes.com*, 6 May 2019. Available at: https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/#ea907b3f8953. See also the IDF tweet at: https://twitter.com/IDF/status/1125066395010699264

It is of course worth asking (but outside the scope of this chapter) why terrorists (as they are conventionally understood) have not managed to pull off a cyberattack of serious magnitude. “I’m as puzzled as you are,” said Michael Hayden, who served as NSA director from 1999-2005 and CIA director from 2004 to 2008. “These folks are not cyberdumb (…) They use the web and show a great deal of sophistication in how they use it, for many purposes (…) But they have not yet used it to create either digital or physical destruction. Others have”. Kathy Gilsinan, ‘Will We see a Terrorist Cyberattack before Midterms?’ *The Atlantic*, 1 November 2018. Available at: https://www.theatlantic.com/international/archive/2018/11/terrorist-cyberattack-midterm-elections/574504/


36 Leyden, John ‘Hack on Saudi Aramco hit 30,000 workstations, oil firm admits’, *The Register*, 29 August 2012. Available at: https://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/

37 Perlroth, Nicole, ‘In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back’, *New York Times*, 23 Oct 2012. Triton, the malware involved in a subsequent 2017 attack against a Saudi Aramco petrochemical facility, which was said to be the first attack to directly target the safety systems of a critical infrastructure facility, was, according to experts, likely created by one or more states, with some suggesting Iran and/or Russia as the possible authors of the virus. Perlroth, Nicole and Clifford Krauss, ‘A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try’, *The New York Times*, 15 March 18; Elias Groll, ‘Cyberattack Targets Safety System at Saudi Aramco’, *Foreign Policy*, 21 December 17. Available at: https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/


44 Stilgherrian, ‘North Korea is the most destructive cyber threat right now: FireEye’, ZDnet, 5 October 2018. Available at: https://www.zdnet.com/article/north-korea-is-the-most-destructive-cyber-threat-right-now-fireeye/


50 Josh Rogin, ‘NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history”, Foreign Policy, 9 July 2012. Available at:


55 For the Atlanta attacks, see Lily Hay Newman, ‘Atlanta Spent $2.6M to Recover from a $52,000 Ransomware Scare’, *WIRED*, 23 April 2018. Available at: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/; and Benjamin Freed, ‘One year after Atlanta’s ransomware attack, the city says it’s transforming its technology’, *Statescoop*, 22 March 2019. Available at: https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/. The attacker demanded a Bitcoin payment roughly equal to $51,000, but it is unclear whether this sum was paid. For a similar ransomware attack against Baltimore in May 2019 that caused approximately $18 million in damage, see Christine Fisher, ‘A ransomware attack is holding Baltimore’s networks hostage’, 8 May 2019. Available at: https://www.engadget.com/2019/05/08/baltimore-city-government-ransomware-attack/#comments


61 *The Convention on Cybercrime of the Council of Europe (CETS No.185).* Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

62 For a useful introduction to some of the issues through the prism of the thinking of a country that has given considerable thought to crucial critical issues, see the Dutch Minister


For an example, see Schmitt, M. ‘The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis’. 


Securing Our Common Future: An Agenda for Disarmament, pp. 56-57. Cyber also features in the implementation plan in the Agenda, in terms of prevention of malicious cyber activity and fostering an adherence to accountability and adherence to international cyber norms. Available at: https://www.un.org/disarmament/sg-agenda/en/  


As one observer has put it, “In many ways, nation-state cyber-wars are already well underway. The lack of established international norms means that many cyber-attacks fall into a grey area below the threshold of total war.” Isaac R Porsche III, ‘Fighting and Winning the Undeclared Cyber War’, 24 June 2019. The Rand Blog. Available at: https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html  


See, for example, Australian Signals Directorate/Australian Cyber Security Centre, Strategies to Mitigate Cyber Security Incidents – Mitigation Details, February 2017. Available at: https://www.cyber.gov.au/sites/default/files/2019-

73 Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau and Rosalie McQuaid, Developing Cyber Resilient Systems: A Systems Security Engineering Approach, NIST Special Publication 800-160, Vol. 2, November 2019, p. xiv. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf. As the authors observe, “Cyber resilient systems operate more like the human body than a finite-state computer. The human body has a powerful immune system that absorbs a constant barrage of environmental hazards and provides the necessary defense mechanisms to maintain a healthy state. The human body also has self-repair systems to recover from illness and injury when defenses are breached. But cyber resilient systems, like the human body, cannot defend against all hazards at all times.” (Op. cit., p.xvi).


75 This can involve discussion and thinking at the very fundamental level: who deals with cyber threats? One authority? Or is an interagency model to be preferred? For some sense of the thinking in Israel which has pondered these questions deeply, and which has gone through various evolutions (and now has a single agency responsible for cyber in the civilian domain, the National Cyber Directorate), see Eviatar Matania, Lior Yoffe and Tal Goldstein, ‘Structuring the national cyber defence: in evolution towards a Central Cyber Authority’, Journal of Cyber Policy, Vol.2 (Issue 1), 2017, pp. 16-25.

76 Many such national frameworks exist – either fully formed or implemented as official strategy, or put forward as conceptual proposals. This author has found particularly useful the framework contained in Eviatar Matania, Lior Yoffe, and Michael Mashkautsan, ‘A Three-Layer Framework for a Comprehensive National Cyber-security Strategy’, Georgetown Journal of International Affairs, Volume 17, Number 3, Fall/Winter 2016, pp. 77-78.


80 Even where the private sector recognizes the need for effective cybersecurity measures and mitigation and is willing to allocate resources to this end, it may still see cybersecurity primarily as an issue of technical protection. A government’s law enforcement arm, however, may have priorities such as the identification of the threat actor. See the trenchant remarks of Myriam Dunn Cavelty and Victor Mauer, ‘Introduction’, in Myriam Dunn Cavelty and Victor Mauer (eds.), International CIIP Handbook Vol.II: Analysing Issues, Challenges, and
Prospects. Center for Security Studies, ETH Zurich, 2006, p. 11. Available at:
https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-security-studies/pdfs/CIIP-HB-2006-2.pdf
84 Vijayan, Jaikumar, ‘What is an ISAC or ISAO? How these cyber threat information sharing organizations improve security’, CSO Online, 9 July 2019. Available at: https://www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html
90 What has been presented above is necessarily a brief treatment of various preparedness, mitigation, and cyber resilience measures. For detailed discussion, see further Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau and Rosalie McQuaid, Developing Cyber Resilient Systems: A Systems Security Engineering Approach, NIST Special Publication 800-160, Vol. 2, November 2019, pp. 10-11.
91 The use of two factor or multi-factor authentication is (for example) not perfect, and there have been an increasing number of sophisticated attempts (including those using social engineering) that attempt to defeat it. See Zak Doffman, ‘FBI Issues Surprise New Cyber Attack Warning: Multi-Factor Authentication Is Being Defeated’, Forbes, 7 October 2019. Available at: https://www.forbes.com/sites/zakdoffman/2019/10/07/fbi-issues-surprise-cyber-attack-warnings-new-precautions/#3ac359b27efb
92 Newman, Lily Hay, ‘Equifax officially has no Excuse’, WIRED, 14 September 2017. Available at: https://www.wired.com/story/equifax-breach-no-excuse/. The US Justice Department in February 2020 charged officers from the Chinese People’s Liberation Army (PLA) for being behind the cyberattack. ‘Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax’, United States Department of Justice, 10 February 2020. Available at:
94 ‘Combating the Insider Threat’, National Cybersecurity and Communications Integration Center, 2 May 2014. Available at: https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf
95 Multidisciplinary teams can also be useful for modelling cyber risk scenarios. See ‘Cyber risk research impeded by disciplinary barriers’ (various authors), *Science*, Vol. 366, Issue 6469, pp. 1066–1069 (29 November 19).
96 For an example of its uses in India, see ‘Ethical Hacking: The Challenges Facing India’, *BBC*, 4 December 2019. Available at: https://www.bbc.com/news/world/asia-india-50583733
99 The Canadian Centre for Cybersecurity also does similar outreach and provision of guidance to the public on cyber threats and cyber hygiene. ‘5 Practical Ways to make Yourself Cybersafe’. Available at: https://www.cyber.gc.ca/sites/default/files/publications/five-practical-ways-yourself-ef.pdf
100 Estonian National Security Concept, 2017, p. 17. Available at: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf. The author is very grateful to Eneken Tikk-Ringas for reading this section and making numerous suggestions concerning Estonian cyber preparedness, which improved the draft immeasurably. Remaining errors are the author’s own.
103 The digital ID system covers every Estonian, but not everyone holds the ID-card or other artefact allowing use of the system. I am grateful to Eneken Tikk-Ringas for enlightenment on this point.
unleashing cyberwar to disable Estonia’, *The Guardian*, 17 May 2007. The initial trigger was the relocation of a statue of a Russian soldier from a prominent place in central Tallinn. The statue represented the Russian state (which had unveiled the statue in 1947) and to the ethnic Russians living in Estonia the Soviet victory over Fascism, but to many Estonians this was seen as a symbol of occupation. The two nights of rioting over the issue (between ethnic Russians and Estonians) on 26 and 27 April 2007 coincided with the beginning of the cyberattacks (on 27 April). The attacks spiked on 9 May (Victory Day, the Russian holiday marking the defeat of Fascism) and 10 May. See Mark Landler and John Markoff, ‘Digital Fears Emerge After Data Siege in Estonia’, *The New York Times*, 29 May 2007. Available at: https://www.nytimes.com/2007/05/29/technology/29estonia.html; and Damien McGuinness, ‘How a Cyber Attack Transformed Estonia’, *BBC*, 27 April 2017. Available at: https://www.bbc.com/news/39655415.


110 Ibid.


For a summary, see:

117 Cybersecurity Strategy 2019-2022. For a summary, see:


122 ‘Estonia’s RIA concludes agreement on enhancement of cyber-security with India’ The Baltic Times, 22 Augustus 2019. Available at: https://www.baltictimes.com/estonia_s_ria_concludes_agreement_on_enhancement_of_cybersecurity_with_india/


124 The center had already been offered to NATO in 2003, but the events of 2007 hastened the process and gave the CCDCOE a great deal more visibility. (Personal communication, Enek Tikk-Ringas, February 2020).

125 Available at: https://ccdcoe.org/about-us


The actual threshold for triggering Article 5 has not (yet) been clearly spelt out, with this lack of certainty owing (at least partly) to difficulties with attribution, and to determining what exactly constitutes a cyberattack of a magnitude that would make an Article 5 invocation an appropriate response. See ‘Nato: Cyber-attack on one nation is an attack on all’, BBC, 27 August 2019. Available at: (https://www.bbc.com/news/technology-49488614) and Jason Healey and Klara Tothova Jordan, ‘NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow’, p.7 (and Box 7). It should be borne in mind that Estonia during the 2007 cyberattacks did not consider itself to be under armed attack and refrained from requesting NATO support under Article 5.

Brent, Laura ‘NATO’s role in Cyberspace’, 12 February 2019. Available at: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

“The CyOC serves as NATO’s theatre component for cyberspace and is responsible for providing cyberspace situational awareness, centralized planning for the cyberspace aspects of Alliance operations and missions, and coordination for cyberspace operational concerns”. Available at: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.


Cf. Available at: https://ccdcoe.org/exercises/locked-shields/

As more cyberattacks loom, Singapore has a weak ‘first line of defence’

Of 2,035 respondents polled for the various milestones in Singapore’s SMART Nation journey, see ‘SMART Nation Progress’. Available at: https://www.smartnation.sg/why-Smart-Nation/smart-nation-progress


139 Cf. Available at: https://www.internet.ee/cif/news/cybernuts-crushed-by-over-9-5000-students-across-estonia. - Separately, there have also been pilot programs ongoing to develop courses in basic cybersecurity that have been conducted in schools. See Kalev Aasmee, ‘Cybersecurity for kids: ‘The earlier we teach this, the better specialists we’ll have’, ZDnet, 24 February 2016. Available at: https://www.zdnet.com/article/cyber-security-for-kids-the-earlier-we-teach-this-the-better-specialists-well-have/


142 ‘ID-kaardi kiibis peitub teoreetiline turvarisk’ (“There is a theoretical security risk in the ID card chip”), ERR.ee. Available at: https://www.err.ee/616719/id-kaardi-kiibis-peekub-teoreetiline-turvarisk

4 September 2017; Hans Lõugas, ‘Riik palub: ID-kaarti saab kääl uuendada, aga ärge tehke seda’ (“The state asks: ID cards can be updated, but don’t do it”), Digigeenius, 26 October 2017. Available at: https://digi.geenius.ee/rubrik/uudis/riik-palub-id-kaarti-saab-kull-uuendada-aga-arge-tehke-seda/; ‘Uuendamata jää 300 000 turvapõlvikega ID-kaarti’, (‘300,000 ID cards with security risks were not renewed’), Pealinn, 2 April 2018. Available at: http://www.pealinn.ee/tagid/koik/uuendamata-jää-300-000-turvapõlvikega-id-kaarti-n218022


145 For the various milestones in Singapore’s SMART Nation journey, see ‘SMART Nation Progress’. Available at: https://www.smartnation.sg/why-Smart-Nation/smart-nation-progress

146 Cf. ‘Transforming Singapore’. Available at: https://www.smartnation.sg/why-Smart-Nation


148 Of 2,035 respondents polled in the Cyber Security Agency’s 2018 edition of its public awareness survey, approximately 34% had stored their passwords in their computers or wrote them down, or used the same password for work and personal accounts. ‘The Big Read: As more cyberattacks loom, Singapore has a weak ‘first line of defence’”, TODAY, 23 Feb 2019. Available at: https://www.todayonline.com/big-read/big-read-more-cyber-attacks-loom-singapore-weak-first-line-defence
150 For some reflections, see Benjamin Ang and Shashi Jayakumar, ‘Smart Nation, but will we be Secure?’, The Straits Times, 14 August 2016. Available at: https://www.straitstimes.com/opinion/smart-nation-but-will-we-be-secure
151 The Strategy has one of its key tenets, strengthening the resilience CII. The others tenets are: (a) mobilizing businesses and the community to make cyberspace safer by countering cyber threats, combating cybercrime and protecting personal data; (b) developing a vibrant cybersecurity ecosystem comprising a skilled workforce, technologically-advanced companies and strong research collaborations, so that it can support Singapore’s cybersecurity needs and be a source of new economic growth, and (c) stepping up efforts to forge strong international partnerships, given that cyber threats do not respect sovereign boundaries. Cf. Available at: https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy; for the full strategy see: https://www.csa.gov.sg/news/publications/~/media/0ecd8f671af2447890ec046409a62bc7.ashx.
152 2016 saw the first attack of any note against CII (in this case, telecommunications) - broadband outages caused by customers’ own virus-infected machines that carried out DDoS attacks on the network of a key broadband provider. - ‘Star hub: Cyber-attacks that caused broadband outages were from customers’ own infected machines’, The Straits Times, 26 October 2016. Available at: https://www.straitstimes.com/tech/starhub-cyber-attacks-that-caused-broadband-outages-came-from-customers-infected-machines. It is possible that the ultimate source of the attack could have been malware-infected devices (such as web cams or routers) that customers had purchased themselves.
153 The 2017 edition of these drills, Exercise Cyber Star held in 2017, was the first such exercise to bring together all agencies responsible for the eleven CII. ‘11 critical information infrastructure sectors tested for the first time in national cybersecurity exercise’, ChannelNewsAsia, 18 July 2017. Available at: https://www.channelnewsasia.com/news/singapore/11-critical-information-infrastructure-sectors-tested-for-first-9040914
156 See for example https://ictconnection.moe.edu.sg/cyber-wellness/cyber-wellness-101
157 Available at: https://www.cyberyouth.sg/ and https://www.csa.gov.sg/programmes/sgcyberyouth


160 ‘MFA’s IT system was breached last year, reveals Yaacob’, TODAY, 11 May 2015. Available at: https://www.todayonline.com/singapore/immediate-steps-precautionary-measures-taken-against-govt-system-breaches-csa

161 ‘Hacking of Mindef system a ‘covert’ attack’, The Straits Times, 4 April 2017. Available at: https://www.straitstimes.com/singapore/hacking-of-mindef-system-a-covert-attack. In 2019, in another attack involving the Ministry of Defense, systems of two vendors working with the ministry were compromised. The data potentially compromised included names, addresses and national identity card numbers of approximately 100,000 military personnel.

162 ‘Personal data of 2,400 Mindef, SAF staff may have been leaked’, The Straits Times, 22 December 2019. Available at: https://www.straitstimes.com/singapore/personal-data-of-2400-mindef-saf-staff-may-have-been-leaked

163 ‘Cyber-attacks on NUS, NTU in bid to steal sensitive data’, The Straits Times, 13 May 2017. Available at: https://www.straitstimes.com/tech/cyber-attacks-on-nus-ntu-in-bid-to-steal-sensitive-data. It appears that an attack discovered in October 2017 against the National University of Singapore, which saw computers of at least two employees at NUS targeted, including a researcher involved in a security project funded by the Ministry of Defense, was distinct from the April attacks. ‘NUS discovered global phishing attack to steal its academic research and data in October’, The Straits Times, 31 October 2017. Available at: https://www.straitstimes.com/singapore/education/nus-targeted-in-global-phishing-attack-to-steal-academic-research


165 It is worth noting that email log-in information (and passwords) of employees of several government agencies featured within a tranche of data found on the Dark Web from 2017-2019. It appears that the leaks did not come directly from government systems, but from public servants’ use of official government email addresses for non-official purposes. Also featuring in the tranche were details of over 19,000 compromised bank payment cards. ‘Email log in details of govt staff put up for sale on Dark Web’, The Straits Times, 22 March 2019. Available at: https://www.straitstimes.com/tech/e-mail-log-in-details-of-govt-staff-put-up-for-sale-on-dark-web

166 ‘Style of SingHealth cyber-attack, info targeted point to state-backed hackers, say experts’, The Straits Times, 22 July 2018. Available at: https://www.straitstimes.com/singapore/style-of-attack-info-targeted-point-to-state-backed-hackers-say-experts. A cyber threat monitoring company, Symantec, subsequently laid the finger of blame on a APT actor, Whitefly, which is “a highly adept group with a large arsenal of tools at its disposal, capable of penetrating targeted organizations and maintaining

167 Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited’s Patient Database on or around 27 June 2018 (10 January 2019), p. 54, p.71 and p. 195. Available at: https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx. In the wake of the IHiS/SingHealth attack, senior officials noted that internet separation should have been implemented at an earlier point in the public healthcare system (just as it had been done in the public sector). ‘Internet separation ‘could and should have’ been implemented in public healthcare system: DPM Teo’, ChannelNewsAsia, 24 July 2018. Available at: https://www.channelnewsasia.com/news/singapore/internet-separation-should-have-been-implemented-teo-chee-hean-10558584

168 The inquiry reached no definitive finding as to how the malicious actor first gained entry into the IHiS system. But on the balance of possibilities, a spear phishing attempt that successfully infected a SingHealth front-ended workstation with malware seems to have been the most likely explanation. Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited’s Patient Database on or around 27 June 2018 (10 January 2019), p.54. Despite the title of the report, the earliest signs of a system compromise in fact dated back to 23 August 2017, with the cyberattack spanning the period 23 August 2017 to 20 July 2018 (Idem, p.51).


170 What has been given above is a sampling of the recommendations. See ‘COI on SingHealth cyber- attack: 16 recommendations’, The Straits Times, 10 January 2019. Available at: https://www.straitstimes.com/singapore/16-recommendations; also Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited’s Patient Database on or around 27 June 2018, pp.221-425.

171 Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited’s Patient Database on or around 27 June 2018, p. 225. A great many of the “technical” recommendations from the COI were not new and were reminiscent of recommendations put forward in other contexts and locations. See for example the US CERT’s 2019 recommendations for IT solutions providers and their customers. Recommendations (which find echoes in the SingHealth COI report) include applying the principle of least privilege to their environment, integrating log files and network monitoring data from IT service provider infrastructure and systems into customer intrusion detection and security monitoring systems for independent correlation, aggregation and detection, and working with customers to ensure hosted infrastructure is monitored and maintained, either by the service provider or the client. Chinese Malicious Cyber Activity. Available at: https://www.us-cert.gov/china
172 For other incidents involving health data in Singapore, see ‘HIV-positive status of 14,200 people leaked online’, ChannelNewsAsia, 28 January 2019 (involving a deliberate leak online of the identities and identifiers of HIV-positive individuals by an individual linked to an “insider”), and ‘Personal information of more than 800,000 blood donors exposed online by tech vendor: HAS’, ChannelNewsAsia, 15 March 2019 (the leak of the personal information of approximately 800,000 blood donors in Singapore in January 2019 after mishandling by a vendor). Available at: https://www.channelnewsasia.com/news/singapore/hiv-positive-records-leaked-online-singapore-mikhy-brochez-11175718 and https://www.channelnewsasia.com/news/singapore/blood-donors-information-exposed-online-hsa-11349308


176 ‘Budget 2020: S$1b to be spent on enhancing Government’s cyber, data security capabilities’, ChannelNewsAsia, 18 February 2020. Available at: https://www.channelnewsasia.com/news/singapore/budget-2020-fund-enhancing-government-cybersecurity-12446336. Specifics programmes and initiatives leveraging on these funds have at the time of writing yet to be announced.


179 The Singapore Board of Directors 2017 survey showed that while cybersecurity is a concern for 9 out of 10 boards in Singapore, it is still not part of strategic discussions at the board level. ‘Cyber security critical concern of Singapore companies but not ranked high in board focus: Survey’, The Straits Times, 7 November 2017. Available at: https://www.straitstimes.com/business/companies-markets/cyber-security-critical-concern-of-singapore-companies-but-not-ranked


181 Opening Remarks by Dr Janil Puthucheary, Senior Minister of State (SMS), Ministry of Communications and Information and SMS-in-Charge of Cybersecurity at the Launch of the Cyber Security Call for Innovation 2019, 2 October 2019. Available at: https://www.csa.gov.sg/news/speeches/cybersecurity-call-for-innovation-2019

182 ‘The Big Read in Short: Singapore’s weakest link in cyber security’, TODAY, 23 February 2019. Available at:


See Weimann, Gabriel ‘Cyberterrorism: The Sum of All Fears?’, Studies in Conflict & Terrorism, 28 (2), pp. 131-134.


The US CERT was also initially set up in partnership with Carnegie Mellon University. Available at: https://www.cmu.edu/cmnews/extra/030915_cyberpartner.html


Cf. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf


Ibid., p. 140.


Ibid.


Ibid.

Statement of Admiral Michael S. Rogers, Commander United States Cyber Command before the Senate Committee on Armed Services, 19 March 2015. Available at: https://fas.org/irp/congress/2015_hr/031915rogers.pdf

Strohm, Chris, ‘Sony hack prompts review of government help in private company security’, Seattle Times, 11 January 2015. Available at:  


See Weimann, Gabriel ‘Cyberterrorism: The Sum of All Fears?’, Studies in Conflict & Terrorism, 28 (2), pp. 131-134.


The US CERT was also initially set up in partnership with Carnegie Mellon University. Available at: https://www.cmu.edu/cmnews/extra/030915_cyberpartner.html


Cf. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf


Ibid., p. 140.


Ibid.


Ibid.

Statement of Admiral Michael S. Rogers, Commander United States Cyber Command before the Senate Committee on Armed Services, 19 March 2015. Available at: https://fas.org/irp/congress/2015_hr/031915rogers.pdf

Strohm, Chris, ‘Sony hack prompts review of government help in private company security’, Seattle Times, 11 January 2015. Available at:


203 Cf. Available at: https://www.nist.gov/cyberframework; Knake, Rob ‘Obama’s Cyber doctrine: Digital Security and the Private Sector’.


208 Engagement with CISA is voluntary, and some have argued that the collaboration between government and the private sector, and the ability to get the private sector to take up CISA’s services designed to prevent and mitigate cyberattacks has been stymied by this lack of regulatory power. See Sam Bieler and Randy Milch, ‘Cybersecurity in One Voice: Leveraging CISA Programming to Improve FTC Cybersecurity Enforcement’, Lawfare, 5 December 2019. Available at: https://www.lawfareblog.com/cybersecurity-one-voice-leveraging-cisa-programming-improve-ftc-cybersecurity-enforcement

209 Available at: https://www.us-cert.gov/nccic


211 Daniel Kaniewski, Building a culture of Cyber Preparedness. Available at:
and director of the National Security Agency, before the Senate Committee on Armed Services, 27 February 2018. Available at: https://www.fifthdomain.com/show-reporter/ausa/2019/10/16/cyber-command-wants-to-work-more-closely-with-the-energy-sector/


The critical infrastructure identified: telecommunications, banking and finance, electrical power, oil and gas distribution and storage, water supply, transportation, emergency services, and government services.


Statement of Admiral Michael S. Rogers, Commander United States Cyber Command before the Senate Committee on Armed Services, 27 February 2018. Available at: https://www.armed-services.senate.gov/imo/media/doc/Rogers_02-27-18.pdf


Statement of Admiral Michael S. Rogers, Commander United States Cyber Command and director of the National Security Agency, before the Senate Committee on Armed
Services, 27 February 2018. Available at: https://wwwarmed-services.senate.gov/imo/media/doc/Rogers_02-27-18.pdf

223 For an assessment of the likelihood of Iranian retaliatory cyberattacks following Soleimani’s assassination, as well as an excellent survey of recent cyberattacks by Iran or its proxies against the United States, see Annie Fixler, ‘The Cyber Threat from Iran after the Death of Soleimani’, CTC Sentinel, February 2020, Vol.13, Issue 2. Available at: https://ctc.usma.edu/app/uploads/2020/02/CTC-SENTINEL-022020.pdf


227 Russon, Mary-Ann, ‘Hackers hijacking water treatment plant controls shows how easily civilians could be poisoned’, International Business Times, 23 March 2016. Available at: https://www.ibtimes.co.uk/hackers-hijacked-chemical-controls-water-treatment-plant-utility-company-was-using-1988-server-1551266


230 Gallagher, Sean, ‘Why the “biggest government hack ever” got past the Feds’, ArsTechnica, 8 June 2015. Available at: https://arstechnica.com/information-

231 Cf. Available at: https://www.us-cert.gov/china


240 Ruiz, Monica M., ‘To Bolster Cybersecurity, the US Should Look to Estonia’, WIRED, 14 February 2020. Available at: https://www.wired.com/story/opinion-to-bolster-cybersecurity-the-us-should-look-to-estonia/

241 Cf. Available at: https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html


Bibliography


Farivar, Cyrus, ‘Cyberwar I: What the attacks on Estonia have taught us about online combat’, Slate, 22 May 2007. Available at: https://slate.com/technology/2007/05/what-the-attacks-on-estonia-have-taught-us-about-online-combat.html


‘Hacking of Mindef system a ‘covert’ attack’, The Straits Times, 4 April 2017. Available at: https://www.straitstimes.com/singapore/hacking-of-mindef-system-a-covert-attack


Singapore’s Cybersecurity Strategy. Available at: https://www.csa.gov.sg/news/publications/-/media/0ecd8f671af2447890ec046409a62bc7.ashx


‘The Big Read: As more cyberattacks loom, Singapore has a weak ‘first line of defence’’, TODAY, 23 February 2019. Available at: https://www.todayonline.com/big-read/big-read-more-cyber-attacks-loom-singapore-weak-first-line-defence


Weimann, Gabriel, ‘Cyberterrorism: The Sum of All Fears?’ Studies in Conflict & Terrorism, 28: pp. 129–149, 2005
Web-based Resources


Canadian Centre for Cybersecurity, ‘5 Practical Ways to make Yourself Cybersafe’. Available at:https://www.cyber.gc.ca/sites/default/files/publications/five-practical-ways-yourself.pdf


Liv, Nadine, United Cyber Caliphate, International Institute for Counter-Terrorism, 20/3/2019. Available at: https://www.ict.org.il/Article/2361/United_Cyber_Caliphate/#gsc.tab=0


Schmitt, Michael, ‘The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis’, Just Security, 14 October 2019. Available at:
https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/
Chapter 30
Prevention of Lasting Traumatization in Direct and Indirect Victims of Terrorism

Shannon Nash

In the wake of a terrorist attack there is an expectation of trauma after such purposeful and unpredictable violence. The nature of terrorism itself perpetuates fear, paranoia, and anxiety. However, there is immense variability in response to trauma, both immediately and over time. Studies on direct and proximal exposure to attacks, as well as individual response to terrorism and indirect exposure, demonstrate that the impact of terrorist attacks is not limited to those directly affected by it. This chapter reviews the findings of important studies and practical efforts to anticipate and reduce risk factors contributing to lasting traumatization of terrorist victims. Several areas of focus emerge in the literature involving major national traumas, first responders, children, the media, and community support. In addition, it is important to understand the experience of others who have faced such trauma and have built resilience. This includes countries which have faced chronic terrorism and decades of war that have left citizens profoundly affected, psychologically and socially. Important gaps remain in our understanding of lasting traumatization in direct and indirect victims of terrorism. This chapter identifies a variety of flexible responses and mental health strategies which include: support for first responders, promotion of resilience in children, media delivery and consumption, and rapidly adapting community-based initiatives. It is a challenge to rely on hypotheticals in disaster planning, but preparation both before and after an attack occurs contribute toward effective, abiding responses that can be built into permanent infrastructures and public health models.

Keywords: healthcare, preparedness, prevention, terrorism, trauma, victims, media, resilience
On 7 August 1998, Mohamed Rashed Daoud al ‘Owhali and Jihad Mohammed Ali (aka Azzam) arrived at the parking lot behind the American embassy in Nairobi, Kenya. When the embassy security guard refused to open the gate al ‘Owhali hurled grenades at him. The guard shouted “Break! Base! Terrorism” in his radio and then he ran, leaving the drop bar down. Azzam fired a handgun toward the embassy in order to draw its occupants to the windows and at one point he began shouting out of the truck window. Al ‘Owhali threw his flash grenades, but the guards refused to open the gate. Without getting past the guards, at 10:35 a.m. Azzam detonated the bomb. The truck was pulled parallel to the embassy and the blast demolished a multi-storey secretarial college and severely damaged the US embassy building and the Cooperative Bank Building. In 1998 the US embassy in Nairobi had about 200 people present at any one time. Most of the people who worked for the embassy were Kenyans, called Foreign Service Nationals. There were also American employees and contractors, part-time employees, and interns, college students, and high school students from a summer hire program. The attack perpetrated by Al-Qaeda operatives killed 213 people, including 44 embassy employees (12 Americans and 32 Foreign Service National employees). More than 4,000 people were injured at the embassy and in the vicinity.

The faces of those persons who ran to the windows after Azzam’s gunshots were hit by broken glass when the bomb went off. US Ambassador Prudence Bushnell described the moments immediately following the blast, saying, “I was thrown back, and although I didn’t think at the time I was unconscious, I must have been because when I brought myself back to reality, I was sitting down with my hands over my head because the ceiling was falling down.” Once out of the building, she described that what she first saw on the street: “A lot of glass, lot of glass, twisted pieces of charred metal…I looked up and saw burning vehicles. I saw the charred remains of what was once a human being. I saw the back of the building completely ripped off, and utter destruction.” According to Donald Sachtleben, chief forensic adviser with the FBI, “The rear of the embassy … was just devastated. Every window was blown out. The cement or brick work that was along the face of the wall of the embassy had numerous places where there appeared to be high velocity impact, that is, there were holes or cracks in the wall. I could see window frames that were just actually twisted right out of the wall itself.”

At the October 2001 sentencing hearing in New York City of the Al-Qaeda perpetrators of the bombings, victim impact statements presented chilling accounts of the trauma inflicted that day and beyond. One of them, Howard Kravaler, testified about recurring “flashbacks of the bombing and my vain attempts to locate my wife’s remains … the carnage of the 11th of September has only served to exacerbate these nightmarish memories.” Frank Pressley was injured in the bombing and he refers to the three years since the attack as “nothing but hell” with health complications and “tremendous nightmares for several years.” Frank’s wife Yasemin, who was pregnant at the time, also worked at the embassy and although she was not injured, she came out of the building to see her husband in unbelievable condition. Frank testified that the years since “have been nothing but a long nightmare” for both of them. Such stories put a human face to the traumatization from exposure to terrorism.

Lee Ann Ross worked at the US Agency for International Development (USAID) in Nairobi in August 1998. She recalls embassy colleagues first fleeing the building to make sure they are alive and then going back in to pull out their dead or injured colleagues. Lee Ann ran the operations center that day and she lost her best friend in the attack. In the aftermath, tasks like going to hospitals to identify the dead and injured and telling distressed relatives by phone who is alive and who is dead were done only by volunteers. “I could never order anyone to do this, knowing the trauma they are about to experience,” she explained. Lee Ann called all of the counsellors she knew in town to ask for help and two regional State Department
psychiatrists arrived the next day. Eventually there was a disaster relief package set up for the Kenyan victims. The adrenaline kept her going for a couple of weeks, then the nightmares started. Working overtime, denial became the antidote. Furthermore, she lamented, “We are asked to do anything and everything, except be victims … (...) The implicit message has been pretty clear, Foreign Service Officers are not supposed to be affected by trauma.” She retired three years later and moved back to the US, went on antidepressants, had a lot of somatization, and began seeing a counsellor again. Years after the bombing, Lee Ann started to deal with the Nairobi trauma.

According to the academic consensus definition, terrorism is “calculated, demonstrative direct violent action” that targets mainly civilians and non-combatants and it is “performed for its propagandistic and psychological effects on various audiences.” Due to the nature of this purposeful and unpredictable violence, the psychological trauma terrorism inflicts is unavoidable. While some of the effects of trauma - like nightmares or flashbacks after an attack like the Nairobi bombings are common, responses can vary over both time and space after such a traumatic event. There is variability in the responses to trauma and the impact of terrorist attacks are not limited to those directly affected by the violence. Terrorism is fear-generating violence. The indirect strategy of terrorism also means that the immediate victim is not the main or ultimate target. As Alex Schmid indicated in the second chapter of this volume, the use of violence against certain individuals or groups serves to intimidate or coerce and, as a message generator, it reaches an audience much larger than direct victims or local witnesses. When exploring “trauma” and “terrorism” Michael C. Frank argues that terror works in the opposite temporal direction of trauma. “Put simply” Frank says, “trauma is the unintentional (re)experiencing of past violence, whereas terror is the fearful anticipation of future violence - based on, and initiated by, the occurrence of violence in the past.” There is infliction of wounds from attacks themselves, but there is also trauma projected forward in the form of scenarios even worse and therefore, as Derrida put it, “the wound remains open by our terror before the future and not only the past.”

It is inevitable that direct and indirect victims of terrorism will have feelings of intense fear and be traumatized. However, the lasting effects of trauma can be softened and even prevented with pro-active and pre-emptive measures to reduce the risks of permanent traumatization of direct and indirect victims of terrorism. This chapter will provide a snapshot of the vast literature on terrorism and trauma and offer a brief overview of important findings. It concludes with a summary of suggestions from the literature with a focus on prevention and preparedness measures that could reduce the lasting effects of trauma in direct and indirect victims of terrorism. This author’s background is in history and it is through an historical and contemporary analytical lens that the study has been conducted. This is not a comprehensive survey of the field of terrorism and trauma, neither geographically nor historically inclusive, however, this chapter synthesizes several important themes that emerge from a selection of studies from the field and brings forward preventative measures informed by the literature. This chapter is informed by, and builds on of the comprehensive scholarship available in The Trauma of Terrorism: Sharing Knowledge and Shared Care, An International Handbook, edited in 2005 by Yael Danieli, Danny Brom, and Joe Sills.

First the chapter begins with a discussion on the variability in response to trauma. A review of the literature informs how we conceptualize victims of terrorism and explore the effects of trauma with direct and indirect exposure. The 9/11 attacks prove to be an important case study here. Next, the chapter looks at cases of repeated chronic terrorism and lessons in resilience. Case studies here include the Al Aqsa Intifada in Israel, ZAKA body handlers, ethnic warfare in Sri Lanka, and Holocaust victims. The final section of this chapter looks at a selection of attempts by relevant experts to address the lasting traumatization of victims, especially the experiences of those who faced trauma and built resilience. A case is made for prioritizing strengthening the resilience and preparedness of potential victims and the employment, social,
and healthcare constructs within which they operate. The author offers suggestions for responses and mental health strategies, including feasible prevention and preparedness measures that have been or can be taken to reduce the risk of lasting traumatization. These suggestions focus on early support for first responders, supporting resilience in children, media delivery and consumption, and community resilience and community-based initiatives. It is impossible to anticipate every scenario in disaster planning, but, in general, responses to terrorism must prepare for phases of response both before and after an attack occurs.

Victims of Terrorism: Direct and Indirect Exposure

On the morning of 11 September 2001, hijackers carrying small knives, box cutters, and cans of mace- or pepper-spray took control of four aircrafts and flew two of them into the North and South Towers of the World Trade Centre in Lower Manhattan and one in the western side of the Pentagon in Washington DC. The fourth plane crashed into a field in southern Pennsylvania after passengers intervened and launched an assault on the cockpit. More than 2,600 people died at the World Trade Centre after both towers collapsed less than 90 minutes after the second impact; 125 died at the Pentagon and 256 died on the four planes. The 9/11 Commission Report - one of the largest criminal investigations in history - refers in its 2004 report to 9/11 as a day of “unprecedented shock and suffering in the history of the United States.” Television coverage of the events that day was immediate, graphic, and pervasive. People not physically present at the scene of crime witnessed on television horrific scenes of airplanes flying into buildings, the towers collapsing, and the aftermath of the plane crashes. Stories of Americans going to work or flying to visit Disneyland when tragedy struck; chilling audio recordings of last phone calls from the airplanes; visuals of unrecognizable first responders covered in dust and debris; videos of individuals jumping from the towers with the reactions of horrified bystanders below; and missing person posters wallpapering parts of New York City.

Empirical information about psychological reactions to 9/11 became available quickly after the attacks. In the days that followed, Mark A. Schuster et al. assessed the immediate mental health effects of the attacks by conducting a nationally representative survey of 560 adults. The interviews surveyed participants’ reactions to the terrorist attacks and their perceptions of their children’s reactions to investigate how people who were not present at a traumatic event may experience stress reactions, thus exploring the effects of terrorism on indirect victims. This study found that 44 percent of the adults sampled experienced at least one of five substantial stress symptoms since the attacks and 90 percent reported at least low levels of stress symptoms. Thirty-five percent of parents reported that their children had at least one of five stress symptoms and 47 percent reported their children worried about their own safety or the safety of loved ones. The study found that adults coped with stress symptoms in various ways such as talking with others (98 percent), turning to religion (90 percent), participating in group activities (60 percent), and making donations (36 percent).

As informed by previous studies of trauma and disaster, “Catastrophes can have a pronounced effect on adults who are not physically present.” In their study, the authors found that the “potential for personalizing the 9/11 attacks was large, even for those who were thousands of miles away at the time. Although the people we surveyed who were closest to New York had the highest rate of substantial stress reactions, others throughout the country, in large and small communities, also reported substantial stress reactions.” This study found that the level of stress was associated with the extent of television viewing (which will be explored later in this chapter) and found that it may have served as a method of coping for some people, but for others, particularly children, media consumption may have exacerbated or caused stress. Furthermore, Schuster et al. explained that many respondents anticipated future attacks and noted that “When people are anticipating disaster, their fears can worsen
existing symptoms and cause new ones.” Roxane Cohen Silver et al. conducted a longitudinal investigation of psychological responses to 9/11, with a US national probability sample, and found significant psychological reactions across the US after 9/11. This study’s findings strongly suggest that substantial effects of the events of 9/11 rippled throughout the country and “many individuals who were not directly exposed to the attacks reported symptoms both acutely and over the year afterwards at levels that were comparable to those individuals who experienced the attacks proximally and directly.” According to Cohen Silver and colleagues, “the requirement of direct and proximal exposure to the attacks and the expectation of a dose-response relationship between exposure and traumatic stress response are myths.”

While there are psychological effects of indirect exposure to mass violence, physical proximity to traumatic events is related to an increased likelihood of experiencing traumatic symptoms. A nationally representative, web-based epidemiological study conducted by William E. Schlenger et al. examined the association between stress symptoms one to two months after the attacks and indices of exposure to the event. This study found that the prevalence of probable Post-Traumatic Stress Disorder (PTSD) “was significantly higher in the New York City metropolitan area (11.2%) than in Washington, DC (2.7%), other metropolitan areas (3.6%), and the rest of the country (4.0%) … However, overall distress levels in the country were within normal ranges.” In a summary of the main findings from the empirical literature that assessed the psychological impact of the 9/11 attacks, Schlenger found that “Initial cross-sectional findings showed that many adults in the US were deeply disturbed by the attacks, but subsequent longitudinal findings suggested that much of the distress documented in the initial assessments was self-limiting (i.e. resolved over time without professional treatment.” According to Schlenger, “studies focusing on clinically significant symptoms and probable disorder prevalence generally showed that probable PTSD prevalence was strongly associated with direct exposure (or ‘connection’) to the attacks, and that the PTSD problem following the attacks was concentrated in the New York metropolitan area.” The studies that retrospectively assessed pre-9/11 exposure to traumatic events also found that such exposure was an important risk factor for developing PTSD after the attacks. Schlenger acknowledges the importance of these initial studies but cautioned that they must be considered preliminary.

In an effort to better understand the lasting traumatization of 9/11, A. Lowell et al. published in 2017 a systematic review of the available longitudinal information about the trajectories of 9/11-related PTSD among exposed populations as a unique data set. Drawing from the work of previous studies, Lowell and colleagues describe PTSD as “a disabling, maladaptive reaction to traumatic stress with significant functional impairment and comorbidity.” The study’s goal was to “clarify the longitudinal prevalence, course, and correlates of PTSD in high-exposure populations during the 15 years since 9/11.” The authors drew a number of important conclusions:

“Overall prevalence of PTSD following 9/11 appears to be relatively high in the period directly following the attacks, particularly for those with the greatest levels of traumatic exposure. These rates appear to decline over time for the majority. The exception is first responders and rescue/recovery workers, who appear to have had lower PTSD prevalence than other populations in the first 3 years following 9/11, but show substantial increase in prevalence after that point.”

Available studies (which are limited) suggest that PTSD rates may peak at five or six years post-9/11 for first responders and rescue/recovery workers. Prevalence of PTSD among non-traditional responders (e.g. volunteers) is markedly higher than for traditional ones (e.g. police and firefighters). Lowell et al. postulate that initially lower rates of PTSD that increase over
time may result from traditional responders’ “resistance to help-seeking behavior and under-reporting, and possibly due to the nature of training and preparedness.” The study also suggests that the higher prevalence of PTSD among non-traditional responders could be explained by lower levels of training and support that leads to greater vulnerability. The study confirmed that exposure intensity is a primary risk factor and, in longitudinal studies involving first responders’ 9/11-related injury and job loss, were identified as important factors in the chronicity of PTSD.

In 2001, and over the following decade, the Diagnostic and Statistical Manual of Mental Disorders (DSM-IV-TR) classified PTSD in the anxiety disorders category and some experts criticized the criteria for exposure to trauma as being too inclusive. Evidence emerged that multiple emotions, like guilt, shame, and anger, placed it outside of the fear/anxiety spectrum. The fifth edition of the Diagnostic and Statistical Manual of Mental Disorders (DSM-5), released in 2013, made the conceptual change of putting PTSD in a new diagnostic category “Trauma and Stressor-related Disorder.” The DSM-5 provides four qualifying exposure types in Criterion A for PTSD: 1) direct personal exposure, 2) witnessing trauma to others, 3) indirect exposure through trauma experience of a family member or other close associate, and, the recently added, 4) repeated or extreme exposure to aversive details of a traumatic event, which applies to workers who encounter the consequences of traumatic events, such as military mortuary workers and forensic child abuse investigators.

Both direct and indirect victims of terrorism are at risk of lasting traumatization, particularly those who meet Criterion A for PTSD in the DSM-5. The DSM-IV-TR (1994 edition) used the phrase “experienced, witnessed, or was confronted with” to refer to three qualifying exposure types, but the ambiguous “confronted with”, in apparent reference to indirect exposure through close associates, has been removed in the DSM-5 exposure to trauma definition. While the DSM-IV-TR “did not specify whether witnessed exposures had to be in person, or whether media reports could constitute a witnessed exposure,” the DSM-5 clearly states that witnessing the trauma of others must be “in person.” Furthermore, the DSM-5 narrows the exposure through media wherein it specifies that the criteria for exposure “does not apply to exposure through electronic media, television, movies or pictures unless it is work-related.” However, using an unspecified definition of witnessed trauma exposure in the years after 9/11, research studies counted media reports, which greatly broadened who could be considered trauma-exposed for the purposes of measuring symptoms.

This chapter will focus more specifically on PTSD, but the psychological effects of terrorism are not limited to PTSD and can include disorders and comorbid conditions, including Major Depressive Disorder (MDD), Generalized Anxiety Disorder (GAD), Complicated Grief (CG), affective disorders, aggressive behavior and conduct problems, substance use, and sub-clinical psychological distress.

The DSM-5 criterion for PTSD includes both direct and indirect as qualifying exposure to types to trauma. For 9/11-related PTSD, the most consistently documented correlates of PTSD across studies were based on exposure to the event. Yuval Neria et al. explain that “In particular, loss of life of significant others, physical injury, and immediate risk of life were especially predictive of PTSD. Therefore, across samples and studies, survivors and direct victims of the attacks were consistently shown to have increased risk of PTSD compared with individuals in the community.” The 9/11 attacks were traumatizing to a great number of people, as the attacks exposed Americans to their vulnerability and the attacks were on a scale few thought possible. Most or all Americans identified with the victims of 9/11 and perceived the attacks as directed at them as well. The psychological effects of the attacks were
exacerbated by recurrent triggers, fears of a second-wave of attacks, and ongoing threats that could be local. Michael C. Frank frames the terror caused by terrorism as “a halfway house between the real (actual attacks and their tangible aftermath) and the imaginary (possible future assaults).” Traumas in general are random, unpredictable and uncontrollable, but terrorism is unique in the way that it adds a faceless enemy, with ideological undertones, whose specific goal is to create ongoing anxiety in the populace. The terror inflicted by terrorism is far-reaching, but the lasting traumatization of direct and indirect victims is centered on highly exposed individuals. As drawn from the DSM-5, those who suffer from PTSD were directly exposed through personal exposure, witnessing trauma to others, indirect exposure through the traumatic experience of someone close to them, or extreme exposure to details of a trauma through work. This chapter focuses on these victims to explore what we can learn from the experience of those who have endured such trauma and found resilience. The main focus is on practical efforts that can aid in the prevention of lasting traumatization.

Repeated Chronic Terrorism and Lessons for Resilience

Studying major national traumas and lasting traumatization begs the question: how do individuals and communities cope with living under the constant threat of man-made violence? There is extensive and important literature on victims of terrorism in ongoing conflict and there is much we can learn from these studies. The following examples have lessons for both resilience (focuses on assets and resources that serve a protective purpose in adverse conditions) and for coping mechanisms (emphasize what a person ought to do when encountering stress). An example of one such study is the work of Eli Somer et al. who examined the 2001-2002 Palestinian terrorist campaign (Al Aqsa Intifada) against Israel’s heartland. It killed over 1,000 Israelis in a prolonged series of terrorist attacks that included shooting incidents, car bombings, and suicide bombings. At the peak of the violence, Somer et al. interviewed citizens residing in areas highly affected by the violence. In line with studies on the psychological responses to the 9/11 attacks, Somer et al. found that “Although citizens residing in the most severely hit locales were also those who suffered most from posttraumatic symptoms, the effects of major national trauma were not limited to those directly affected by it”, further suggesting “that objective measures of exposure or loss may not be sensitive predictors of reactive distress.” The authors explain that little is known on the effects of repeated disasters on the mood of the general citizenry. In their study, Somer et al. found that national mood or demoralization appeared to be unrelated to the level of exposure to terrorism in Israel. Furthermore, those traumatized directly were no more likely to develop a negative mood than other citizens. However, the study found that, counter-intuitively, the mood was not worse in the hardest-hit parts of the country but rather among the interviewees sampled from a remote region in Israel, namely the desert resort city of Eilat. The authors posit that national identification with the suffering in Israel’s heartland, exposure to media coverage of events, combined with an economic crisis in the resort city and less social solidarity and community cohesion, may have contributed to this outcome.

An interesting finding emerged from a study conducted by Zahava Solomon and Rony Berger on ZAKA (Hebrew initials for “Identification of disaster victims”), a voluntary religious organization that is part of the Israeli rescue forces that played a prominent role in body removal and first aid treatment in the aftermath of the Al Aqsa Intifada terrorist attacks. The authors found “a very low level of psychological distress among ZAKA volunteers” with only 2 percent reporting post-traumatic symptoms. Their findings “negate the notion that ZAKA rescue workers are at increased risk for psychopathology” and “suggest that despite their intense and repeated exposure, these men are particularly resilient.” Solomon and Berger suggested several factors accounting for this finding. First, ZAKA work involves recurrent exposure to horrific scenes, but there are also positive feelings that stem from
altruistic and religious extrinsic rewards. Second, self-esteem, and perhaps the promotion of resilience, are reinforced by the respect and admiration bestowed on ZAKA volunteers. Third, their work is strictly voluntary and it is likely that the most resilient volunteer for such a tough mission. Finally, the possibility that the volunteers are sensation and action seekers that have few other outlets besides ZAKA.\textsuperscript{72} In terms of coping mechanisms, the authors found that ZAKA volunteers reported extensive use of religious coping (religion acting as a stress buffer). Looking across different studies, Solomon and Berger explained that “religious coping may exert its beneficial effects through three general pathways: beliefs that may facilitate cognitive restricting of the meaning of the traumatic events, the social support of the close-knit religious community, and a sense of divine control over the stressful experiences.”\textsuperscript{73} ZAKA volunteers also used the coping technique of denial, “which is defined as an unconscious attempt to reject unacceptable feelings, needs, thoughts, wishes, or external reality factors.”\textsuperscript{74} Although denial is, at times, an inappropriate mode of coping, Solomon and Berger found that denial helped contain anxiety and served as a useful protective measure by blocking our information that is too affectively stimulating or anxiety provoking.\textsuperscript{75}

Although there are cases of resilience in case studies of chronic terrorism, the detrimental effects of repeated attacks on individuals, families, and communities cannot be understated. Daya Somasundaram studied victims of terror in Sri Lanka who were profoundly affected psychologically and socially after two decades of inter-ethnic insurgency and counter-insurgency. Collective trauma is a cumulative effect of terror on a community and Somasundaram explained that “given the wide-spread nature of the traumatization due to war, the individual’s psychosocial reactions may have come to be accepted as a normal part of life. But at the community level, manifestations of the terror can be seen in its social processes and structures.”\textsuperscript{76} However, the author indicates that some cultural coping strategies that led to survival during intense conflict may not be adaptable during subsequent peace and reconstruction phases. For example, a deep suspicion and mistrust of others developed among Tamils.\textsuperscript{77} Although there were overwhelming negative consequences to sustained terrorism on the community, in particular a deterioration in values and ethics, Somasundaram described a few positive developments, including emerging grass roots community organizations, the decline of the caste system, and the changing status of women. Furthermore, he says that community level approaches and interventions (e.g. awareness programs, training for grass-roots workers – basic psychosocial skills, rebuilding of community structures, efforts to address social justice and socio-economic rehabilitation) could reverse the worst effects of collective trauma and go a long way in restoring war-torn societies.\textsuperscript{78}

As a final example, in a retrospective study of forty-year follow ups of survivors of the Holocaust and other genocidal tragedies, Henry Krystal investigated “what attributes made individuals able to survive and master the potentially lethal trauma, and what characteristics favored successful resumption of ‘normal’ life?”\textsuperscript{79} Krystal acknowledged that the variety of experiences during the Holocaust were enormous and depending on the challenges an individual faced, inherited personal traits, assets, and patterns of behavior influenced the success of his/her/their efforts.\textsuperscript{80} He goes on to explain that a “healthy infantile feeling of omnipotence is the most important asset for dealing with life’s stresses and potential trauma … It is the emotional mainspring of extraordinary reserves.”\textsuperscript{81} In fact, Krystal claimed that all resilience is built on adult residuals of infantile omnipotence feelings, which are a conviction of one’s security, lovability, and safety.\textsuperscript{82} For survivors of the Holocaust, “unconscious and repressed memory traces are not preserved intact but are subject to complex modifications” and “being able to use disavowal and repudiation (primary repression) and to suspend all mourning was essential.”\textsuperscript{83} “In the concentration camps”, Krystal explained, “even though there was significant traumatization, there were individuals who, with luck and health, were able to establish a pattern of living that they accepted as being a greatly abnormal, but temporary, situation.”\textsuperscript{84} He noted that “As long as they maintained such hope, their degree of
dehumanization was moderated. Hidden vestigial optimism permitted some limited alertness and initiative, even inventiveness.”

Similar to the denial required for the ZAKA body handlers, some victims of the Holocaust used such psychological mechanisms to frame their reality and operate within it. Neria et al. highlights that researchers have identified several factors associated with effective coping during exposure to trauma and reduced psychopathology in its aftermath, including personality traits such as attachment style and hardness, cognitive attributional style, next to a range of biological factors.

The examples above emphasize the traumatic effects of terrorism on individuals, communities, and whole societies. These cases offer insights into survival, coping mechanisms, and resilience. Psychologists define resilience “as the process of adapting well in the face of adversity, trauma, tragedy, threats or significant sources of stress – such as family and relationship problems, serious health problems, or workplace and financial stressors.”

Fostering resilience is at the core of the prevention and preparedness suggestions that follow. Resilience involves, to a certain extent, “bouncing back” from difficult experiences, but it can also involve personal growth. Adverse events do not have to determine the outcome of one’s life, as there are many aspects of life that one can control, modify, and grow with. That is where resilience comes in because becoming more resilient not only helps individuals, families, communities, and societies get through difficult circumstances, but it can also empower growth and improvement of life along the way.

Snapshot of Prevention and Preparedness Suggestions

In their work on mental health and refugees, Miller and Rasco draw a parallel between the problem of smoking and lung cancer and that from a public health perspective it makes good sense to prioritize the prevention of lung cancer through smoking prevention and cessation programs. They go on to frame the following ecological principles:

> “Whenever possible, prevention should be prioritized over treatment, as preventative interventions are generally more effective, more cost-efficient, and more humane than an exclusive reliance on the treatment of problems once they have developed. This does not negate an important role for treatment; it simply regards individual treatment as one tool in the arsenal of intervention responses.”

In Chapter Two of this Handbook, Alex Schmid poses the question: “Should we be concentrating on reducing the capabilities of terrorists, or diminish their motivations or should we be prioritizing strengthening the resilience and preparedness of their potential victims and targets?” This chapter postulates that building resilience and preparedness play a significant role in diminishing the effects and probability of lasting traumatization in direct and indirect victims of terrorism. In a study conducted by Stevan E. Hobfall et al., the authors assembled a panel of experts on the study and treatment of those exposed to trauma to gain consensus on intervention principles. They “identified five empirically supported principles that should be used to guide and inform intervention and prevention efforts at the early to mid-term stages.

These are promoting: 1) a sense of safety, 2) calming, 3) a sense of self-and community efficacy, 4) connectedness, and 5) hope.” They frame the guidelines as particularly important for broader public health and emergency management. The authors make an important call for more broad-scale interventions that ought to be available to large numbers of individuals quickly, which “means that intervention must not only be conducted by medical and mental health professionals, but also by gatekeepers (e.g. mayors, military commanders, school teachers) and lay members of the community.” In addition, Hobfall and colleagues emphasize that “Stopping the cycle of resource loss is a key element of intervention and must become the
focus of both prevention and treatment of victims of disaster and mass trauma, and this includes loss of psychosocial, personal, material, and structural (e.g. jobs, institutions, organizations) resources.\textsuperscript{94}

The principles laid out by Hobfall et al. are important guides for promoting resilience and focusing on prevention of lasting traumatization by means of interventions that go beyond the bounds of psychotherapy. Resilience is fostered in individuals, the wider-work or social community, and the larger population. Preparedness before a traumatic event intends to cushion the effects of the psychological stress and promote resilience. What follows is a snapshot of prevention and preparedness suggestions highlighted in a sample of the literature on trauma and terrorism that focuses on four specific groups or themes: 1) supporting first responders, 2) promoting resilience in children, 3) media delivery and consumption, and 4) community initiatives. A review of the practical efforts at preventing and managing trauma and loss derived from the literature informs the suggestions around comprehensive and flexible responses and mental health strategies. Such intervention and prevention measures have to work collaboratively with proper access to mental healthcare, early identification of risk factors, integrated medical screening, and education and intervention efforts aimed at public safety and healthcare professionals. If mental health disaster planning and preparedness can be built into permanent infrastructures, effective response capability will endure an emergency.\textsuperscript{95}

The suggestions here are drawn from the literature, but Hobfall et al. remind us that it is “critical that we remain modest in our claims about what interventions can accomplish towards prevention of long-term functional and symptomatic impact … it is unknown to what extent such interventions will be associated with significant improvements in functioning.”\textsuperscript{96} What follows indicates primary prevention efforts (interventions implemented prior to the onset of symptoms and as a protection against harmful events before they produce dysfunction) and secondary prevention efforts (implemented after trauma exposure and aims to curtail dysfunction, disorder, or pathology).\textsuperscript{97} While there is an emphasis on primary prevention suggestions, secondary interventions are included as a way to effectively inhibit lasting traumatization. Furthermore, operationalizing the prevention and preparedness suggestions explored below should be designed to fit the specific needs to the culture, place, and type of trauma. They should also be tested, refined, and re-evaluated.

**Supporting First Responders**

Law enforcement officers, ambulance personnel, firefighters and other emergency-response workers are often the first to respond to terrorist attacks that are distressing and horrific by design of the perpetrators. This can precipitate a traumatic response that may negatively affect their physical and mental health.\textsuperscript{98} There is an important body of psychological research on the effects of trauma on front line officers and it suggests that there are major negative consequences of unresolved trauma. These consequences include a higher prevalence of alcoholism, serious illnesses related to stress, isolation, family difficulties, lowered concentration, sleep disturbances, difficulties in concentration, eating excessively, gambling, unsafe sex, and attempted or completed suicide.\textsuperscript{99}

Part of the day-to-day duties of first responders is attending to critical incidents. Support for their mental and physical health must already be built into their training. Furthermore, traumatic incidents accumulated through a career are, as a whole intertwined and unified, shaping the complex form of trauma. Therefore direct or indirect exposure to trauma is not the only factor that may lead to a later experience of trauma.\textsuperscript{100} In a study of police officers, Chistiane Manzella and Konstantinos Papazoglou discuss “that the law enforcement field is characterized by a unique form of subculture, the so-called ‘police culture’ which often prioritizes physical strength for the survival of the officers on the street.”\textsuperscript{101} While this culture enhances solidarity and cohesion, the open expression of fear or emotions in response to
charged events is often held unacceptable and considered weakness in police culture. First responders have the unique positions of dealing with horrific events at one moment then needing to calm, console, and take charge, and while emotional responses are inherent in these responders, ignoring them comes at a high price of reduced quality of life and well-being. One challenge is the idea that trauma happens to others and “not me” and that first responders are supposed to protect and take care of victims, rather than becoming victims themselves, which goes against their sense of identity. In order to support, educate, and help first responders the literature highlights several areas of focus that will now be discussed.

**Police Culture**

Manzella and Papazoglou found police educators to be in a unique position to address the issue of “police culture” and senior officers who carry out the training are in a unique position to help the next generation of officers to be cognizant of the ways to handle exposure to trauma and loss. They can encourage police officers to see themselves as possible victims and/or survivors of terrorism and can work to create bridges with mental health professionals. This comes in the form of resilience promotion programs (which have been successfully applied to US army military personnel). Such programs should not only be instituted and promoted to assist rookie officers and personnel, but senior first responders serve to benefit as well. Breaking the stigma associated with reaching out for help (which is often paired with unsought negative changes in job duties or reduced pay) is essential to providing support for first responders.

**Journaling**

Training modules with proven success have helped police officers improve their well-being and stress resilience through relaxation techniques and visual imagery exercises. Practical exercises in training include: psycho-education about trauma, mindfulness/ awareness training called “be where your feet are” and journaling. Police trainee participants in one study reported that they were more comfortable writing than talking; writing in journals also helped participants organize their memories. There is also a desire to link mindfulness-awareness with procedures in the field, based on the ability to “check the reality of where you are and who you are” which often prevents negative effects often experienced in the aftermath of trauma, like disassociation.

**Peer-counselling**

Organizations (those who hire, train, support, and oversee) first responders should develop necessary interventions to provide responders with appropriate tools and coping mechanisms for their complex and cumulative form of trauma. As one study on police officers noted, “Thereby, police organizations would become a type of protective milieu that apply such programs and train their personnel so that police officers would be more resilient in dealing with the exposure to different threatening situations.” Studies have found peer-counselling effective; those providing the support ought to be directed by guidelines from mental health professionals.

**Practice-based Treatment**

Continued and new conversations among mental health professionals and first responder
organizations. This would help “the development of a practice-based multifaceted treatment that would enable mental health professionals to respond to police officers’ and their families’ needs more effectively, considering the multitude forms of police trauma and its consequences in the police organizations.” As discussed by Konstantinos Papazoglou, clinicians will then be able to view police trauma as a cumulative product, formed by critical incidents and multiple factors rather than a single traumatic event that triggered symptoms. Job-related PTSD can be further complicated by a child abuse history and significant dissociation or mood dysregulation.

**Treating PTSD**

In terms of treatment to mitigate the lasting effects of trauma, Nina F. Lewis-Schroeder et al. discuss PTSD treatment in first responders in the form of a four-phase approach used in the McLean Hospital LEADER program: Phase 1: Diagnostic assessment; Phase 2: Symptom stabilization and skills training; Phase 3: Trauma-focused processing; Phase 4: Consolidation and aftercare. Peter T. Haugen et al. also describe an integrative approach for the treatment of PTSD in 9/11 first responders that is built around three core techniques: 1) Meaning making: engaging the patient in meaning making regarding the traumatic experience; 2) Following the affect: bringing about a situation where the patient spends sustained periods of time focusing on the source of the distress; 3) Interpreting defenses: interventions that address avoidance strategies. In addition, studies have explored the merits of Cognitive-Behavioral Therapy (CBT) for treatment of PTSD in first responders.

**Female First Responders**

Research also draws attention to special considerations for female first responders. One study cautions that numerous factors need to be kept in mind for the treatment of female first responders, “including their potentially different attachment styles from male first responders and also the likelihood of their having relational versus individualistic coping styles.” Lewis-Schroeder et al. found that “Successful treatment is best achieved through person-centered care and careful attunement to both the stated and inferred individual goals of the patient.” It can be assumed that multiple factors are also at play for the treatment of LGBTQ, minorities, and others with diverse experiences and backgrounds.

**Family Support**

Research indicates that there is a “buffering” effect of social support on risk for PTSD. It underscores the importance of preventative efforts to increase family and work social support during disaster response and recovery. Such support may help mitigate the harmful effect of trauma, as well as other risk factors, and promote resilience. The support of spouses, family, religion and/or faith, a sense of community support for first responders, and a prepared team of mental health professionals ought to work together to buffer the risks.

**Pre-incident Training**

Those who administer first responder programs should recognize the resilience of first responders while also acknowledging the importance of emotional and psychological support sources for building and maintaining that resilience. Efforts should be made to reinforce and strengthen such sources before a terrorist incident occurs, including family programs in
departments, recognition of the role religion and/or faith plays—perhaps through a volunteer or official chaplain’s office, and mental health professionals gaining the trust of first responders before an incident to strengthen support during and after.127

Promoting Resilience in Children

Terrorism affects children directly and indirectly around the world. Millions are exposed to traumatic events and the broad, severe, and long-term impacts on our society are yet to be fully understood.124 While it has been stated that the majority of children are resilient and able to cope, many children need some kind of structured intervention.125 In particular, preschool children (ages 0-6) are passing through critical developmental stages, which makes them more vulnerable to trauma than older children. Research indicates that their exposure to terrorist incidents and disasters may drastically influence their health and further development.126 Studies after terrorist attacks (including Oklahoma City, New York, Israel, and elsewhere) have shown that 10-16 percent of adults and children suffered from chronic PTSD that caused significant difficulties in their functioning. However, only a very small number of people, especially children, received psychological treatment in the sub-acute and chronic stages.127

While older children were more likely to meet the criteria for conduct disorder or depression, younger children were more likely to have PTSD, agoraphobia, and separation anxiety. Children who were personally exposed to the event or had family exposure were at a greater risk for PTSD.128 Furthermore, Annette M. La Greca and Wendy K. Silverman emphasize in their work that “children and adolescents exposed to disasters and acts of terrorism are likely to need more than interventions that focus exclusively on PTSD reactions because their reactions are often complex and multifaceted and may include other problems (such as grief, depression, and anxiety).”129 To promote resilience in children, Leo Wolmer, Daniel Hamiel, and Nathaniel Laor suggest that “stress inoculation as a way of primary prevention might be a cost-effective strategy.”130 There is a general consensus that protective factors and those that promote resilience include self-esteem, coping strategies, social support, hope and meaning, optimism, and humor.131 Several studies identify teachers and the education system as an important resource for building resilience in children, due to their daily contact and ability to provide direct and ongoing support. Parents and caregivers are of course a vital component of promoting resiliency, as they buffer and translate terrorist acts to children.

In order to promote resilience and support children (and their families) exposed to trauma, the literature highlights several areas of focus.

Parent-Child Relationship

Enhance the readiness of children and their families by increasing their resilience prior to a terrorist attack. This is promoted by an early history of secure attachment fostered by consistent and supportive care, which can have a powerful and enduring influence on children’s adaptation and has been shown to increase the likelihood they will utilize formal and informal support at later stages.132 Especially in the formative years, a child’s development is intimately connected to parent functioning and parent reactions are important to understanding children’s adaptation.133 Understanding the impact of terrorism and children’s responses to exposure must include viewing children in the context of their families. As Pfefferbaum et al. explains, “Children are greatly affected by parental support and intervention and by the larger ‘recovery environment’ in the aftermath of trauma, including terrorist assault. Over time, parents’ ability to manage their own responses and to support their children’s processing of events will influence the child’s adjustment.”134 Pfefferbaum and her colleagues acknowledge that terrorism creates independent health and psychological effects on parents and they call for
more work on the impact of terrorism and the parent-child relationship/parenting to identify risks and implications of preparedness.  

School-Training in Preparedness

Mental health interventions that can be delivered in community settings to children and adolescents can help provide effective preparedness for children to cope with traumatic events. Schools can play a central role as the de facto provider of mental health services. The study by Wolmer, Hamiel, and Laor focused on teacher-based initiatives for building resilience among Israeli children exposed to ongoing attacks. This research “demonstrated that a teacher-mediated, protocol-based intervention focused on resilience enhancement is an effective method to grant students coping skills to help them face daily stressors and transfer the knowledge to cope with severe life events, process them, and recover swiftly to regain normal routine.” The intervention in this study was implemented three months before the traumatic exposure and found “significant difference in symptoms of post-trauma and stress/mood among participants and control children.” Furthermore, “the effects of the teacher-delivered intervention go beyond reduction in trauma symptoms and include the enhancement of coping and adaptation in general.” Another study by Daniel Hamiel et al. said that “Kindergarten-based universal preventive interventions seem promising, non-stigmatic, and cost-effective.”

Providing Psychoeducation

Interventions among masses of students can be facilitated through a shift in the role of education. Teacher-led interventions in the study by Wolmer, Hamiel, and Laor aimed at enhancing children’s resilience by:

“(1) providing psychoeducation to understand and normalize stress reactions; (2) addressing (identifying and replacing) dysfunctional thoughts and beliefs that mediate development of psychological symptoms, for example that the world is completely dangerous; (3) learning to manage anxiety and regulate emotions, understanding and better controlling the interrelationship between thoughts, feelings and behaviour; (4) teaching problem-focused coping and imaginal exposure (to develop perspective taking, self-talk, and positive imagery); (5) encouraging students to increase activities that foster positive emotions; (6) facilitating social support and sustained attachments (to build on and enhance existing support and lasting relationships, e.g. effective listening); and (7) instilling hope to counteract the shattered worldview and the vision of a shortened future characteristic of mass trauma.”

The focus is on building resiliency and strengthening resources (rather than direct processing of traumatic experiences). This approach avoids difficulties in program adherence and the need for individual attention, particularly in regions where exposure to terrorism is direct, intense, and wide-ranging.

Training Trainers

Training for education professionals, such as the National School Intervention Project (developed in Israel in October 2000 in response to high levels of stress experienced by civilian population), specifically the “Building Resilience: A Program for Teachers and Students” facet
of the program. A parent component offered at schools was an integral part of the project. Naomi L. Baum provides an in-depth look at such a program and explains that classroom activities were centered on the themes of a) Relaxation; b) Exploring Fears in particular, and Feelings, in general; c) Building of Resources; and d) Finding Hope and Meaning in Difficult Situations.\textsuperscript{142} Baum concludes that “Empowering teachers through workshops that provide information, skills, confidence-building activities, and support turns teachers into natural partners of mental health professionals working in schools, and creates an environment that can support resiliency and wellness among the student body.”\textsuperscript{143}

\textit{School-based Activities}

Restoration of the school community as an essential step in re-establishing a sense of self-efficacy through support, school-initiated social activity, and learning opportunities, including an opportunity for children to see grief appropriately modelled, as well as participate in the planning and implementation of activities.\textsuperscript{144} This can also include programs that reduce disparities in schools by providing support for parents and enriching early learning opportunities for economically disadvantaged children. This approach has produced positive effects on cognitive skills.\textsuperscript{145}

\textit{Recognizing Post Traumatic Stress Disorders (PTSD)}

Parents and school communities working with mental health professionals to intervene as soon as symptoms appear. Physicians, psychologists and other clinicians may be able to help people identify normal stress reactions and encourage steps to cope effectively. This also involves educating parents on what signs to look for in their children and how to respond to their needs.\textsuperscript{146} A dialogue between mental health professionals with an expertise in PTSD and primary care physicians should be open to integrate screening for PTSD into general medical practice. This could come in the form of self-administered screening tools, educational brochures, and effective communication to increase detection, enhance appropriate referrals to specialists and improve clinical management of patients with psychiatric symptoms.\textsuperscript{147} Primary care providers are in the unique position that they may be the first to recognize symptoms and recognize when those with a PTSD diagnosis are entering a related psychosocial crisis.\textsuperscript{148}

\textit{Media Delivery and Consumption Practices}

The spread of fear to trigger emotional and behavioral reactions are hallmarks of terrorism, as are “lasting psychological distress and counteractions driven by emotions rather than by substantiated consideration.”\textsuperscript{149} How leaders, the media, communities, and societies react to terrorism, and its underlying threats, plays a role in how terrorism is perceived and how fear is instrumentalized. Such fears are dramatically spread through mass and social media. Michelle Slone and Anat Shoshani highlight that “The primary goal of terrorism is the creation of fear and intimidation. To this end, the media is frequently exploited as a conduit to produce indirect victimization.”\textsuperscript{150} In the case of the 9/11 attacks, news coverage was visceral. People watched terror unfold on live television and were exposed to replays of the carnage over and over again. The media play an important role in the way terrorist acts are broadcasted, explained, and digested by audiences. Media coverage can trigger and exacerbate symptoms of those suffering psychological stress from trauma exposure. Sensationalized media reporting and social media posts can inhibit efforts at resiliency and serve secondary purposes of financial gain and brand exposure for those broadcasting it. Not only does it serve a key purpose of the terrorists, but today’s mass media and social media also play a role in sabotaging prevention and
preparedness efforts aimed at building resiliency. In order to better manage the spread of fear, foster resilience, and discourage the use of the media for terrorists to exert mass psychological impact, the literature highlights several areas of intervention.

**Media Guidelines**

Guidelines and agreements should be considered between the media and the government and among the media themselves. Gabriel Weimann poses some of the basic questions about covering terrorist events, including these: how should such terrible events be reported? And who decides where to draw the line between informing and intimidating the public? How much live coverage should there be? According to Weimann, “The lessons of direct feed, straight from the terrorist scene, have sparked a debate about the impact of such violent and disturbing images, identification of victims on television before informing the relatives, inaccurate reports on the number of victims, and the spread of panic.” This is even more problematic in the age of smartphones and social media. Agreeing to predetermined ethical media principles and adhering to self-imposed guidelines, based on empirical findings, will help establish optimal ways of maximizing security and minimizing the damage from the free flow of (dis-)information in times of terror.

**Removing Hate Speech**

The onus continues to be on social media platforms and their users to report and remove illegal hate speech and work to fight the spread of fake news and misinformation.

**Protecting Children**

Media exposure to terrorism has been found to constitute a significant stressor and studies have found a substantial correlation between media exposure and PTSD in children in particular. Parents are advised to limit their children’s television and social media consumption during a crisis and discuss the event with them. Slone and Soshani also provide the guideline that “Particularly important would be extension of these strategies to children by constructing school curricular programs that address coping with media exposing incidents of trauma and terror.”

**Crisis Lines**

The media has some responsibility to alert viewers to the severity of imminent exposure, this can include a warning sign to identify sensitive and disturbing material, as well as suggesting coping strategies and publicize avenues for help and support, like crisis lines or websites.

**Responsibility of Journalists**

Journalists play the conflicting roles of citizen and journalist while navigating the clash between care for victims and duty to report. In the coverage of terrorism, personal responsibility must be allocated to the discretion of reporters, photographers, camera operators, and editors in the field who are regulating material with a sensitivity to viewer effects.
**Freedom from Fear vs. Freedom of Expression**

Considerations are needed to balance the psychological impacts of media reporting on terrorist events and the danger of restrictions imposed on the freedom of the press and freedom of expression.\(^{158}\) Fear generated by terrorism can be (and has been) manipulated by politicians to pass questionable legislation that undermines civil rights and liberties that under different circumstances would not have received public acceptance.\(^{159}\)

**Responsible Media Coverage**

Gina Ross suggests that by “Adding healing aspects to coverage, such as how people cope and care, the media can help reassure and promote hope and meaning.”\(^{160}\) Media activities can work to protect the public from second-hand trauma and inform and encourage the public by shifting “from the trauma vortex into the healing vortex.”\(^{161}\) Ross provides several activities designed to aid in this shift, including:

1. Frontline media professionals monitor their own levels of stress and learn to safely discharge traumatic energies.
2. Asking questions like: Have we balanced the coverage of the trauma vortex with coverage of the healing vortex?
3. Warning viewers of upcoming disturbing sounds and images.
4. Recognizing the impact of language on a public in shock.
5. Encouraging viewers to watch news in small doses.
6. Avoiding excessive gory details.
7. Avoiding repetitive showing of traumatic images, which can be triggers for painful recollections.
8. A heavy focus on negative news reinforces fears and desires for revenge.
9. Normalizing initial traumatic response and cautioning about the characteristics of unresolved trauma (trauma impairs the ability to think clearly).
10. Providing information on cutting-edge coping and healing methods and working with trauma experts.
11. Informing the public of help available during and after trauma exposure.
12. Running information on emotional first aid.
13. Inserting images of inspiring acts of kindness, compassion, courage, and perseverance.
14. Continued reporting of individual group recovery to help communities overcome feelings of helplessness and regain hope.\(^{162}\)

**Community Resilience and Community-Based Initiatives**

The term resilience is often used in the context of disaster and refers, inter alia, to an individual’s capacity to rebound following experiences of adversity.\(^{163}\) According to Jack Saul, “Researchers and practitioners have increasingly come to see that resilience of an individual does not exist in a vacuum – it is a function of one’s social and cultural content.”\(^{164}\) This is commonly referred to as “community resilience”, which Saul defines as “… the collective capacities in families, communities, organizations, and society at large that are more than the sum of individual capacities.”\(^{165}\) Jack Saul and Judith L. Landau further elucidate that community resilience is “A community’s capacity, hope and faith to withstand major trauma and loss, overcome adversity, and to prevail, usually with increased resources, competence, and connectedness.”\(^{166}\) Building such resilience can be difficult, especially if it is not done beforehand, but it is fundamentally important in trauma preparedness and in the prevention of
long-term psychological and social difficulties. As Danielle Knafo notes, “Human-made violence is something that we need not only to overcome and survive but also to make sense of. By maintaining hope and creating meaning, we can determine the outcome of our survival and, more importantly, our will to live and the quality of our lives.” Learning within a new situation, creating new frameworks for intervention, and implementing programs that are outside of the traditional social services environment can support a transformation from a challenge to an opportunity for growth. According to Jonas Waizer et al. “most crisis counselling experts agree that it is as important to strengthen community support networks as it is to respond to individual need.” Resilience, especially aided by community-based initiatives and family/social circles, is a common theme for both treatment of, and preparedness for the psychological effects of terrorism. As Waizer and his co-authors succinctly note, “Even when the impact is broad, disasters are local events.” In order to better equip communities to foster resilience while rapidly adapting in the wake of terrorist events, the literature highlights the following areas of focus.

**Lessons Learned**

Lessons learned after the 9/11 attacks by the Federation Employment and Guidance Service (F.E.G.S.) – one of New York’s largest community-based not-for-profit agencies – are discussed in an article by Jonas Waizer and colleagues. From this experience, they explain that “F.E.G.S. believes that community agencies must be better prepared to provide quality services at lower cost, and to assess rapidly an emerging situation, possess the confidence to overcome bureaucratic barriers, demonstrate a willingness to experiment with new approaches and discard what is not working.” Community supports should prepare for agile responses and organizations (like F.E.G.S.) can build an infrastructure based on partnerships with other non-profits as well as private and for-profit affiliates. Shared infrastructure is essential to non-profit agencies and an important factor in the response to terrorism and the development of services.

**Offering Help after Terrorist Events**

In the example of F.E.G.S. in New York, Waizer et al. found lessons in blending a public health model, a capacity to respond quickly in a time of crisis, adapt rapidly to new contracts for staffing and technology, and approaches to staff training that are a more flexible mix of mental health practice and public health outreach. There are shame and economic limitations that restrict some individuals from seeking help after terrorist events. The authors found that “By working within communities to build future resilience and assisting in rebuilding and strengthening their own networks, we were able to reach and help with both behavioral and employment services many people who would otherwise have gone unattended.”

**Response Readiness**

Community preparedness and response system coordination includes extensive collaboration “across culturally and organizationally disparate systems such as law enforcement, emergency management, public health, clinical laboratory, mass media, education agencies, and medical response systems from all levels of public enterprise.” Dori B. Reissman and colleagues indicate that “Since emergency response is coordinated at a local jurisdictional level, community preparedness is a key ingredient for homeland security. Response readiness needs to consider both individual and collective behavior and function within the social and cultural contexts of impacted communities.”
Sharing Experiences

Determining the needs of different groups, including local residents, business leaders, school officials, and foreign-born communities and addressing them in preparedness and healing capacities. For example, this means addressing the needs of those who have survived traumatic experiences like escaping war-torn countries may be deeply re-traumatized or minorities may be targeted by racial bias, as stigma raises concerns at the community level. Community support groups bring together neighbors to talk and share experiences, such as a “Time to Share” community support group for lower Manhattan that was established after 9/11 and residents continued meeting for nearly two years.

Strengthening Social Cohesion

The unpredictable violence of terrorism evokes fear, paranoia and chaos. Reissman et al. postulate that “Activities that promote a sense of community well-being and social cohesion would thus be effective countermeasures to this disruption.” Public health strategies should account for the effects of terrorism on social connectedness and “adopt broad interventions that recognize the interdependence of community health and social connections.” The authors suggest that “Community-based settings, particularly those experienced in the health care of special populations, may be better positioned to link victims with family and community networks and resources, especially to reach populations that would not otherwise seek and accept support.”

Family and Community Interventions

Judith L. Landau places an emphasis on the role of the family as a core component in dealing with the effects of trauma. She explains that “facilitating family, cultural, and community ties and enhancing access to family and community resources can be protective against the impacts of trauma. Such connectedness fosters resilience and reduces the short- and long-term effects of stress in families and communities.” She explores the Linking Human Systems Models as an overall approach to guiding family and community interventions to promote healing and reconnection by accessing inherent strengths within families and communities. The core philosophy of the models “is that building a sense of continuity from past to future helps people navigate the present with greater awareness of their choices.” A long-term vision Landau proposes, with the collaboration of international scholars who are involved in communities affected by war, disaster, and mass trauma, to develop “a multi-phased and multi-component tiered system of interventions that integrates: (a) an individual evidence-based intervention; (b) a parenting intervention; (c) a family-level intervention; and (d) a community-level intervention.”

Collective Recovery

Recovery from collective trauma involves collective processes of readjustment, adaptation, and recognizing and strengthening adaptive capacities for resilience in both families and in communities. Jack Saul aptly states:

“These capacities for recovery may be enhanced through the structure and support provided by outside practitioners, may be initiated from within communities themselves, or may be driven by various insider/outsider collaborations. Adaptation following massive traumatic events requires
flexibility responding to changing circumstances over time and at the same time developing a positive vision of recovery. Thus, collective recovery is a creative and emergent process; its content and form are constructed over time and through cycles of collective action, reflection, and narration.”\(^{187}\)

Capacities for resilience are also strengthened by incorporating local values and beliefs regarding psychological wellbeing into the design, implementation, and evaluation of interventions at the community level.\(^{188}\) This serves to increase the likelihood that interventions will be culturally appropriate and therefore increase the odds of program utilization and effectiveness.\(^{189}\)

**Conclusion**

Terrorism involves random victimization and comes unexpected, and the arbitrary nature of this blind violence affects the psychological and mental health of direct and indirect victims. The emotional reaction and high impact of terrorism, especially national traumas, are not limited to the communities directly affected. The social, political, emotional, and economic effects are widespread and long-lasting, which determines how individuals, families and whole communities cope. Studies that look at the psychological impact of exposure to the 9/11 attacks have shown that substantial effects of the attacks rippled through the American society. These affected many individuals who were not directly exposed to the attacks; they too experienced psychological stress symptoms. Indirect exposure to terrorism can result in substantial psychological effects, but physical proximity and direct exposure to the terrorist crime scene result in an increased likelihood of experiencing major trauma symptoms. In the case of the 9/11 attacks, the most consistently documented PTSD cases related to the attacks were correlated to degree of exposure to the event. Therefore, lastingly traumatization of direct and indirect victims is focused largely on highly exposed individuals -- those who were directly exposed through personal presence, witnessed trauma to others, were indirectly exposed through the traumatic experience of someone close to them, or were exposed to details of traumatic events repeatedly through the nature of their work. Case studies of those who experienced repeated or even chronic terror, such as those who witnessed the suicide bombings during the Al Aqsa Intifada in Israel, ZAKA body handlers, inter-ethnic war in Sri Lanka, and Holocaust victims emphasize the traumatic effect of terror on individuals, communities, and nations. The psychological impact of chronic trauma is difficult to understand for most outsiders, but offer those who study it insights into survival, coping, and resiliency that can help future victims when translated into training programs.

Core purposes of terrorism -- to create and instrumentalize fear, panic and chaos in society -- are undermined if a community is able to cope with the psychological trauma induced by acts of terrorism in a way that mitigates emotional damage and encourages proportionate, thoughtful reactions.\(^{190}\) This chapter discussed several ways how societies can support those at risk of lasting traumatization by identifying prevention and preparedness practices and suggesting secondary interventions with favorable results based on various historical and contemporary settings. These suggestions are drawn from practical efforts and findings explored in the literature on support for first responders, promotion of resilience in children, media delivery and consumption, and community resilience and community-based initiatives. A focus on timely prevention and solid preparedness measures can build resilience and enable individuals and communities to withstand adversity and prevail while mitigating the risks of lasting traumatization for those most impacted by campaigns of terrorism or single acts of terrorism.

The studies examined in this chapter offer important pieces of the puzzle; they allow us a better understanding of terror and trauma. The research cited has laid a solid groundwork for
further analysis in the field. Future developments will hopefully continue to explore resiliency with an emphasis on building social cohesion not just in the wake of an attack, but as a preparedness measure. An emphasis on building mental health planning and preparedness into permanent infrastructures to promote effective response capability can offer a hopeful avenue into a future where terrorism terrorizes less.

Dr. Shannon Nash is the Postdoctoral Network Manager of the North American and Arctic Defence and Security Network (NAADSN). This collaborative network provides timely, relevant, and reliable expert advice on North American and Arctic defence and security topics. Shannon Nash is a Research Fellow at Trent University with NAADSN and has ongoing projects at the University of Waterloo, examining education and training in national security and counter-terrorism in Canada and exploring how the “terrorism” label is informed and applied to violent attacks in Canada. She received her Ph.D. in History from the University of Toronto with a focus on 20th century American history, terrorism, and international relations. She studies past and present terrorist threats and attacks as well as Canadian, American, and international defence, security and counterterrorism policies. Shannon’s doctoral thesis focused on the reality of al Qaeda espionage methodology and how the idea of a sleeper agent was perceived and adapted to fit the terrorist threat posed by al Qaeda from the 1990s onwards.
Endnotes

2 Ibid.
5 Ibid., 1852:21.
8 United States of America v. Usama bin Laden, et al., 1858:25.
9 Ibid., 1861:22.
14 Ibid., 95:10-14.
16 Ibid., p. 242.
17 Ibid.
18 Ibid.
19 Ibid., p. 242-243.
20 Ibid., p. 243.
22 Ibid.
24 Schmid, Alex P., “Terrorism Prevention: Conceptual Issues (Definitions, Typologies and Theories”); in: The Handbook of Terrorism Prevention and Preparedness, ICCT, 2021, Chapter 2; See also the “Triangle of Terrorism” on p. 22.


55 Ibid., p. 3.
56 Ibid.
57 Ibid.
59 Pai et al. 2017, p.3.
63 Ibid., p. 1507.
64 Frank 2015, p. 92.
65 Cohen Silver 2005, p. 130.
66 Baum, Naomi L., “Building Resilience: A School-Based Intervention for Children Exposed to Ongoing Trauma and Stress”; in: The Trauma of Terrorism: Sharing Knowledge and Shared Care: An International Handbook, p. 487.
68 Ibid., p. 179.
69 Ibid., p. 178.
71 Ibid.
72 Ibid., p.599-600.
73 Ibid., p. 601.
74 Ibid.
75 Ibid.
76 Somasundaram, Daya, ‘Short- and Long-Term Effects on the Victims of Terror in Sri Lanka’; in: The Trauma of Terrorism: Sharing Knowledge and Shared Care: An International Handbook, p. 221.
77 Ibid., pp. 221-222.
78 Ibid., p. 226.
80 Ibid., p.68.
81 Ibid.
82 Ibid., p. 67.
83 Ibid.
84 Ibid., p. 73.
85 Ibid.
87 “Building Your Resilience”, American Psychological Association, 1 February 2020. Available at: https://www.apa.org/topics/resilience
88 Ibid.
89 Ibid.
91 Ibid.
93 Ibid., p. 301.
94 Ibid.
95 Sederer, Lloyd et al., ‘Challenges of Urban Mental Health Disaster Planning’; in: The Trauma of Terrorism: Sharing Knowledge and Shared Care: An International Handbook, p. 704.
96 Hobfoll 2007, p.301.
99 Ibid., p.105.
101 Manzella 2014, p.103.
102 Ibid., p.104.
103 Ibid., p.105.
104 Ibid., p.106.
105 Ibid.
107 Manzella 2014, p. 106.
108 Ibid., p. 111.
109 Ibid.
110 Papazoglou 2013, p. 205.
111 Ibid.
112 Ibid.
113 Ibid., p.206.
115 Ibid.
119 Ibid.

Schorr, John K. and Angela S. Boudreaux, ‘Responding to Terrorism in the USA: Firefighters Share Experiences in Their Own Words’; in: The Trauma of Terrorism: Sharing Knowledge and Shared Care: An International Handbook, p. 588.


Vardi, Moshe, ‘Identification and Follow-Up by Primary Care Doctors of Children with PTSD After Terrorist Attacks’; in: The Trauma of Terrorism: Sharing Knowledge and Shared Care: An International Handbook, p. 554.

Pfefferbaum 2005, pp. 311-312.


Wolmer et al. 2011, p. 346.

Baum 2005, p. 494.

Hamiel et al. 2017, p.3.

Pfefferbaum 2005, p.314.

Ibid.

Ibid.

Ibid.

Wolmer et al. 2011, p. 345.

Ibid.

Ibid., p. 346.


Wolmer et al. 2011, pp. 346-347.

Ibid., p. 347.

Baum 2005, p. 494.

Ibid., p.496.

Hobfoll 2007, p.294.

Hamiel et al. 2017, Daniel, p.3.


Vardi 2005, pp.555-556.

Ibid., p. 556.


Slone and Shoshani 2010, p.440.


Ibid., p. 389.

154 Slone and Shoshani 2010, p. 447.
155 Ibid.
156 Weimann 2005, p. 386.
157 Slone and Shoshani 2010, p. 447.
159 Ibid.
161 Ibid.
164 Ibid.
165 Ibid.
169 Ibid., p. 509.
170 Ibid., p. 511.
171 Ibid., p. 508.
172 Ibid.
173 Ibid.
174 Ibid., p. 510.
175 Ibid., p. 511.
177 Ibid., p. 709.
179 Ibid., p. 501.
180 Reissman 2005, p. 713.
181 Ibid., p. 718.
182 Ibid.
184 Ibid., p. 9.
185 Ibid., p. 21.
187 Ibid., p. 2.
188 Miller and Rasco 2004, p. 43.
189 Ibid.
190 Bakker and Veldhuis 2012, p. 2.
Bibliography


‘Building Your Resilience’, American Psychological Association, 1 February 2020. Available at: https://www.apa.org/topics/resilience


Ross, Gina. “Guide: Media Guidelines: From the ‘Trauma Vortex’ to the ‘Healing Vortex’”, pp. 391-394; in: Yael Danieli, Danny Brom, and Joe Sills (eds.) The Trauma of


Web-based Resources

American Psychological Association. Available at: https://www.apa.org/
Anxiety and Depression Association of America. Available at: https://adaa.org/
Canadian Psychology Association. Available at: https://cpa.ca/
Canadian Resource Centre for Victims of Crime. Available at: https://crcvc.ca/
International Society for Traumatic Stress Studies. Available at: https://istss.org/home
Office for Victims of Crime: Helping Victims of Mass Violence and Terrorism. Available at:
https://www.ovc.gov/pubs/mvt-toolkit/
National Center for PTSD. Available at: https://www.ptsd.va.gov/
National Child Traumatic Stress Network. Available at: https://www.nctsn.org/
National Institute of Mental Health. Available at: https://www.nimh.nih.gov/
UNODC The Doha Declaration: Promoting a Culture of Lawfulness, Victims of Terrorism
Module. Available at: https://www.unodc.org/e4j/en/terrorism/module-14/key-
issues/effects-of-terrorism.html
Chapter 31

Prevention of Public Panic in the Wake of Terrorist Incidents

Juan Merizalde, John D. Colautti, and James J.F. Forest

Public panic in the wake of a terrorist incident is counterproductive, providing benefits only to the perpetrators of the incident as well as those who seek to capitalize on fear and panic for their own purposes (often political or profit-oriented). And when people panic, they make bad decisions. Fortunately, scholarly research has shown that panic is the exception rather than the norm. Instead, studies of public behavior following natural disasters and terrorist incidents emphasize that most people are rational thinking and logically reacting beings who tend not to panic or to be frozen in fear. Thus, positive outcomes can be expected from devising and implementing research-based strategies that will diminish the likelihood of panic in the wake of terrorist attacks. For example, research on community resilience indicates that being well prepared, effectively communicating accurate, relevant information and empowering citizens to take recommended actions all help to significantly reduce fear and anxiety in times of crises. Following a review of this research, the chapter will conclude with a brief discussion on research policy implications.

Keywords: communication, community resilience, emergency preparedness, empowerment, fear, panic, social trust
There is an assumption - believed by many members of the public, and encouraged by Hollywood shows and politicians - that mass public panic is the most likely response to a major terrorist incident. And yet, scholarly research frequently concludes the opposite: beliefs that we should expect panic are not based on a significant amount of empirical evidence, but can instead be described as “disaster myths.” Further, as one study noted, “These myths matter, for they can serve as rationales for inappropriate, inefficient and even dangerous forms of emergency planning and response.” Rather than expecting irrational panicking and civil disorder, researchers in social science, disaster management, and public health have found that mass behavior in times of emergency is often characterized by a type of resilience that can be facilitated by public policies and practices.

This chapter will begin by examining the pervasive myth of public panic in the wake of a terrorist incident, and the ways in which terrorist networks try to provoke fear and panic as core elements of their strategy - the use of violence to achieve political goals. The chapter will also draw from research in psychology, sociology, security studies, and emergency preparedness to identify evidence-based strategies for preventing panic before, during, and after a terrorist incident - with a particular focus on practical ways to strengthen community resilience. Three areas of activity are particularly important: preparation, communication, and empowerment. Research also illustrates the vital importance of social trust - something that is jeopardized in societies where political polarization is more common than unity. A divided public consistently quarreling amongst themselves is unlikely to come together effectively in times of crisis. Thus, new research-based initiatives are needed to strengthen bonds of trust among community members, as well as between governments and citizens.

The chapter then concludes by examining a variety of research questions that remain unanswered, particularly regarding what data should be collected in order to assess levels of resilience in a society. Similarly, it is still unclear what kinds of efforts to build resilience actually have a positive impact. Without identifying exemplary best practices, it will be impossible to determine whether particularly effective initiatives and programs in one context can be successfully transported for implementation in other contexts. The policy implications of this research for governments and societies worldwide are fairly intuitive. The more a society commits itself to learning about and developing resilience, the more likely it will respond to any kind of terrorist incident in a positive manner, without any of the panic or disorientation that the terrorist might hope to create. This, in turn, means that community resilience can become a deterrent against terrorism: the more resilient a society proves to be in the face of a terrorist threat, the more likely a terrorist network will recognize the futility of its efforts. Thus, bolstering community resilience can be seen as a key component of any successful counterterrorism strategy.

**Research on Fear, Panic and Terror**

Fear is a complicated and powerful emotion that can be stimulated by any number of things in our lives. While many researchers have sought to determine the origins and science behind fear, there is only limited agreement amid a wealth of unanswered questions. We know in general that a complex array of sensors in the brain are primarily responsible for triggering the fear emotion, and that most often the reaction of fear is automatic - that is, we do not consciously choose whether to fear or not to fear. We also know that there is a wide variation from person to person in what causes fear. For some people, a spider or rodent could be the cause of fear, while for others it could be speaking in front of a large audience, and some people have a deep fear of aviation transportation or large bodies of water. Our reactions to fear also vary widely, in some cases evoking nervous laughter while in other cases initiating a “fight or flight” response. Further, researchers have found that the biochemical dimensions of fear - which can include increased heart rate and a rush of adrenaline - are fairly similar across all
people, while the emotional responses to fear are highly personal and varied, with some people enjoying scary movies and extreme sports much more than others.

Psychological, scientific, and medical researchers who study fear routinely describe it as a normal human reaction to specific situations or conditions in which we perceive risks and dangers. Our survival instincts are necessarily intertwined with our ability to sense and fear danger, and to act accordingly. However, each of us has our own unique relationship with this emotion. Personal tragedies and other experiences may lead some individuals to be more fearful in general (e.g., of the unknown and the unknowable), while similar experiences may lead others to become more hardened and less fearful. A person’s fear can also be influenced by a range of formal and informal types of information - for example: government warnings about an impending terrorist attack or natural disaster, horror movies, personal superstitions, religious beliefs, or even just a friend or neighbor who shares with you some scary rumor.

From the research on fear, we can derive a generally accepted definition of the term panic as “an acute fear reaction marked by a loss of self-control which is followed by non-social and non-rational flight.” Panic is different from a “fight or flight” impulse when facing perceived threats to one’s safety - in fact, that impulse is a natural product of human evolution, without which our ancestors may not have survived. It is not necessarily considered panic when someone flees the site of an incident where danger is clearly manifested, or (for example) in the aftermath of a terrorist attack where death and destruction are visibly prominent. Rather it is completely rational (from a self-preservation standpoint) to want to put distance between yourself and such danger or carnage. You are simply and quickly assessing a clear and present threat in your environment, and taking appropriate self-protection measures.

Meanwhile, terror is a state of mind that can undermine rational assessment and response to dangerous situations. It is closely related to panic in a conceptual way, in that the strongly felt emotions of terror may be induced by violent trauma, and the behaviors associated with both panic and terror appear similar. According to Alex Schmid, terror is “created by a level of fear that so agitates body and mind that those struck by it are not capable of making an objective assessment of risks anymore.” Provoking terror among a target population is a central element of a terrorist strategy. Here, the perpetrators of the terrorist acts seek to shock and intimidate the target, disorient and demoralize a society, and coerce them into behaving in ways that are meant to benefit the terrorists. Thus, the links many draw between terrorism and panic in the wake of an attack are seemingly intuitive.

Frequently, three kinds of general assumptions are often made about how people will respond to a terrorist incident. According to research by Perry and Lindell, “conventional wisdom holds that typical patterns of citizen disaster response take the form of panic, shock, or passivity.” Other researchers have also identified basically the same three assumptions about behavior following a terrorist attack: they will flee in panic; they will be frozen in a debilitating state of shock; or they will act in some type of irrational, fear-driven manner that will likely require the intervention of someone else. Drawing from the disaster response literature, specific assumptions have included that communities will witness increased levels of antisocial behavior; victims will become dependent on outside response organizations; evacuation orders will result in a mass exodus; public shelters will quickly fill up with dazed and confused survivors; price gouging, looting and other forms of criminality will be widespread; and it will become necessary to declare martial law to impose order on the chaos. As Webb observes, “perhaps the strongest and most enduring myth of human response to disaster is that the social structure breaks down under stress - victims engage in panic flight with no regard for social relationships, and emergency workers abandon their occupational roles to be with family members.” Recognizing and actively addressing and evaluating these myths should be a cornerstone of any public education effort to ensure a more positive and productive response to the threat of terrorism.
Of course, certain kinds of terrorist attacks will undoubtedly inspire more fear among the target population than others. For example, the detonation of a nuclear bomb is often considered one of the worst-case scenarios because of the destructive capacity of such weapons. While to date no such attack by non-state actors has occurred, it has been featured in many popular fiction books, Hollywood movies and television shows. Similarly, an attack using a contagious virus to intentionally infect a large portion of a population has been portrayed as inciting panic, where the fear of being infected will drive some to behave in irrational (and likely counterproductive) ways. But here as well, no terrorist group has ever come close to the threshold of capability for carrying out such an attack. More realistic, instead, are the suicide bombs and improvised explosive devices that have become a staple in the modern era of terrorist attacks. And even more likely still are assaults with knives and guns, driving cars and trucks into crowds, or hijacking and kidnapping for ransom (or demands to release imprisoned comrades).

The nature of the target attacked by the terrorists also impacts the level of fear among a target population. For example, when the terrorist group attacks a specific type of religious institution (like a Sikh temple) or medical facility (like an abortion clinic), it may have a limited impact on the wider population who are not associated with such targets. In contrast, attacks against public spaces (hotels, cafes, shopping centers, office buildings, sports arenas, etc.) and public transportation (e.g., subways, airplanes, or commuter railways) raise the level of perceived threat among the broader population because virtually anyone could be a victim of such an attack.

Overall, there is a broad spectrum of terrorist attacks, and thus an equally broad spectrum in how individual members of the public may be expected to respond to any particular incident. And unfortunately, there have been so many terrorist incidents over the past half-century we now have a fairly significant amount of data and evidence to analyze how people react in the wake of these attacks. For example, we know that the potential effects on victims of terrorism may be experienced at many interrelated levels - individually, collectively, and societally. According to Erez, there are three circles of ‘personal victimization’ which are determined in accordance with their proximity to the direct victim: “primary or first order victimization, experienced by those who suffer harm directly, whether it is injury, loss or death; secondary or second order victimization, experienced by family members, relatives or friends of primary victims; and tertiary or third order victimization, experienced by those who observe the victimization, are exposed to it through TV or radio coverage of the victimization, or help and attend to victims.”

Studies have found that perceptions about the risks of terrorism may be influenced by the degree to which individuals feel they have knowledge of and control over an outside event, and how familiar and catastrophic the event will be. People are more likely to feel that an activity or event is not dangerous if they can control it. However, researchers have also noted that survivors of terrorist acts may experience fear, shock, anxiety, shame, guilt and self-blame, anger, hostility, rage and resentment, together with a sense of disempowerment and helplessness. Meanwhile, societies may suffer collective trauma, particularly when attacks are targeted against a particular group or community. According to Butler et al., terrorism can uniquely disrupt societal functioning, as it “has the capacity to erode the sense of community or national security; damage morale and cohesion; and open the racial or ethnic, economic, and religious cracks that exist in our society, as evidenced by an increase in hate crimes following the September 11, 2001, attacks.”

Overall, terrorism impacts people and societies in many ways. And fear is embedded in the fabric of terrorism; there can be no terror without the underlying element of fear. However, there are important factors to be considered when assessing the likelihood of sheer panic in the wake of a terrorist attack. To begin with, scholarly research on human behavior under emergency conditions does not support the popular perception that most people respond to
disasters in a socially disorganized or personally disoriented manner. Instead of shock reactions, or panic flight, research has repeatedly demonstrated that individual reactions to natural disasters or terrorist attacks in public spaces are mainly rational, and that most people tend to act in what they believe is their best interest, given their limited understanding of the situation. One study found that public behavior in the immediate aftermath of a major disaster is generally pro-social as well as rational. Following the impact, uninjured victims are often the first to search for survivors, care for those who are injured, and assist others in protecting property from further damage. Further, people who are far away from the disaster scene often donate significant amounts of money and supplies, and are generally willing to offer whatever kinds of assistance they can.

Case studies and ‘after action’ reports of recent incidents illustrate these kinds of behavior. One study found that the evacuation of the World Trade Center in 1993 was tense but orderly. Published reports about the immediate aftermath of the 9/11 attacks also noted the evacuation process of the two WTC towers was orderly and calm, with survivors recounting numerous acts of heroism. The immediate response to the 9/11 attacks also included an influx of volunteers from many parts of the country to assist in clearing the rubble of the World Trade Center and to search for survivors. While there was considerable uncertainty and apprehension during this period, reports of panicked behavior were quite rare. In Tokyo, when the religious cult Aum Shinrikyo attacked subway trains with Sarin nerve agent in March 1995, personal accounts provided by commuters on these trains revealed no real sense of panic during the attacks, with individuals responding in an orderly fashion as they were evacuated from the affected areas. The same behavior was reported in hospitals where victims waited patiently to be treated. Following the July 2005 bombing attacks in London, according to Sheppard et al, “First-hand accounts given in media interviews suggest that the public responses could be better characterized by themes of cohesion, unity, and mutual cooperation, than by any sense of panic.”

These and other examples reflect what research on collective behavior has generally concluded: in the immediate wake of a terrorist attack, members of the public are fairly resilient, calm, and rational in their reactions. According to these studies, “the typical response is marked by the maintenance of normative expectations and role relations. Social order does not break down, and in the case of evacuation, there is no unregulated competition for exits.” Evidence-based research on this topic has demonstrated that “in the face of disaster, most people do not engage in the barbaric, selfish, unthinking, emotional and often self-destructive behavior depicted in the media.” In fact, contrary to expectations of panicked behavior, researchers have noted a tendency for people to redefine norms for social behavior in the wake of a terrorist attack in ways that make helping others an expectation rather than an exception to the norm. As Webb notes, “new norms emerge to govern behavior, and people make every effort to maintain social bonds even under extreme stress.” Further, studies have found that the immediate response period of natural and technological disasters is socially organized, and communities experience an increase in prosocial behavior.

Although it is rare for people to panic, researchers have identified several conditions that must occur - in many cases simultaneously - in order to provoke this kind of behavior: the perception of immediate and severe danger; the existence of a limited number of escape routes; the perception that the escape routes are closing, necessitating immediate escape; and a lack of communication about the situation. Essentially, the literature in this field emphasizes that people confronting a disaster usually react in intelligent, rational ways based on the information they have available to them at any given moment. People often fear what they do not know or do not understand, and panic most often results from fear when there is a paucity of clear and actionable information available. Further, fear and anxiety often diminish a person’s ability to figure out the most optimum response to complex, unfamiliar problems, and the less we understand something, the greater our perceptions of risk tend to be.
Further, a person’s response to a terrorist incident is largely based on what they believe to be true at the time, which may or may not be rooted in factual evidence. This has significant implications in today’s modern social media-infused era, where the tools of influence warfare and disinformation are used to manipulate beliefs, perceptions and behavior in ways that may benefit a political agenda but prove disastrous for the broader society. When our perceptions of risk are misinformed and manipulated, we are unlikely to make the kinds of decisions that will be the most beneficial. Thus, to minimize counterproductive behavior among individuals in a society, it is vital to devise and implement strategies that will prevent or diminish the likelihood of panic in the wake of terrorist attacks. Further, based on the research findings that panic is a considerably less likely response to terrorist attacks than is frequently assumed, it should be intuitive that strategies can be pursued to minimize this even further.

**Strategies to Prevent or Diminish Panic in Emergencies**

Research-based strategies and policies on preventing public panic in emergencies emphasize the essential importance of community resilience, although different definitions of this term are used. For the purposes of this discussion, we can define resilience as the ability to make adaptive processes to alleviate stress by modifying various capacities to restore a level of normalcy in the face of trauma, tragedy, and threat. To put more simply, resilience is “the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.” Several countries—including Australia, New Zealand, the UK, and the US—have formally identified the need to nurture resilience as part of an overall strategy for national security. For example, the 2010 US National Security Strategy describes several essential elements for building resilience: reduction of vulnerability at home, effective management of all-hazards, empowering communities and engaging citizens, building partnerships, and encouraging resistance to fear and overreaction. Similarly, the 2017 US National Security Strategy identifies a series of goals and initiatives meant to strengthen the country’s “ability to withstand and recover rapidly from deliberate attacks, accidents, natural disasters, as well as unconventional stresses, shocks, and threats to our economy and democratic system.”

In the UK, many regions have established “Community Resilience Teams” with representatives from local emergency response authorities and private sector—and several major cities (including London, Bristol, Manchester, and Glasgow) have created the new position of a “Chief Resilience Officer.” These kinds of national strategies inform efforts at the local level to build community resilience as a central means of preventing public panic in the wake of a terrorist incident.

In general, community resilience is seen as a means of mitigating the discomfort of uncertainty. Inherent uncertainty surrounds us all, as a part of life. Individuals, organizations, and governments respond by seeking to manage uncertainty, and reduce it whenever they can. The central goals of any strategy to prevent panic must address the need to reduce uncertainty and instill confidence that no matter what the future holds, the community will make it through. Trust in government— as well as trusting each other— is essential for instilling such confidence, and by extension, community resilience. Further, research shows that higher levels of generalized social trust before exposure to terrorism are linked to lower levels of fear after the event. So, strategies to prevent or diminish panic should include a central goal of increasing trust between the government and society’s various communities, citizens and residents. To this end, three themes of particular relevance appear most prominent in the research on decreasing uncertainty and increasing community resilience: preparation, communication, and empowerment.
Preparation

To be (or at least to feel) completely prepared for any type of unforeseeable event is surely rare. However, a combination of historical analysis and contemporary risk assessment has led to a fairly solid understanding of effective incident preparedness. When considering ways to prepare a society for coping with a terrorist attack, much of our understanding draws from the large literature on preparation for natural disasters. Here, scholars have emphasized the importance of stockpiling emergency supplies and materials; establishing a robust, multi-channel communications infrastructure; and having some form of an integrated system for responding to emergencies, with a clearly defined chain of command and well-defined jurisdictions, legal authorities and responsibilities. In addition, as organizational readiness is broadly seen as a critical component of an effective response to a terrorist attack, a variety of drills and exercises should be conducted to test the response capabilities of emergency services, and remedy any identified concerns or areas of weakness.

Research on best practices for emergency preparedness has informed the development of numerous national-level disaster preparedness plans, several of which focus prominently on fostering resilience for community members and critical infrastructure. For example, Australia’s Strategy for Disaster Resilience describes how individuals and communities “should be self-reliant and prepared to take responsibility for the risks they live with. For a resilient nation, all members of the community need to understand their role in minimizing the impacts of disasters, and have the relevant knowledge, skills and abilities to take appropriate action.”37 Similarly, the 2017 US National Security Strategy emphasizes the need to “build a culture of preparedness and resilience across our governmental functions, critical infrastructure, and economic and political systems.”38 The US Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) are the government organizations primarily responsible for ensuring preparedness at all levels. In addition to gathering and storing emergency supplies at locations around the country (the Strategic National Stockpile), and conducting regular training exercises for first responders, the federal government also provides financial support for local communities to purchase equipment and signage for evacuation routes, among other necessities.

Often, these kinds of preparedness efforts are meant to influence the population’s trust that federal and local government agencies are ready to respond effectively to whatever might happen in the future. A government’s preparedness measures must be matched by public confidence in those measures. There is thus an important perception factor in all of this, which underscores the need for transparency and accountability on the part of government agencies, and for involving ordinary citizens in preparations for natural disasters and terrorist incidents. To that end, national preparedness strategies also emphasize the need to get the public involved, and for every citizen to take some responsibility for personal and family preparations. For example, the American DHS/FEMA sponsors the “Ready.gov” public education initiative which encourages US businesses, communities, families, and individuals to prepare themselves for disasters of all kinds.39 Guidance is provided for effective emergency planning, with a particular emphasis on assembling a personal or family emergency supplies kit (with food, water, first aid, medicines, and other necessities) to ensure their survival for at least a few days. To the degree that the population of a country takes heed of this sort of guidance and prepares accordingly, the research literature indicates we should anticipate lower levels of panic in the wake of a disaster (or terrorist attack).

Communication

A second theme in the research literature on preventing public panic addresses the need for effective communication. In their analysis of research on public responses to terrorist attacks,
Durodie and Wessely made a compelling argument for the need “to identify and prepare mechanisms for accurate and effective dissemination of necessary information through the full range of available media.” It is widely understood that communicating accurate information in a timely manner is a key part of any strategy to reduce fear and panic in the wake of a terrorist incident (or any other crisis or emergency). People look to authorities to help them make correct decisions, and when there is a lack of communication (or authorities are simply not forthcoming with enough information), it can lead to bad decision-making and other negative behaviors. In fact, as Perry and Lindell argued, a lack of information has been found to increase fear in the immediate aftermath of a traumatic incident.

But even before an incident occurs, there must be continual and effective communication between authorities and citizens. In February 2019, the US National Governors Association published a *Guide to Homeland Security*, in which state leaders are encouraged to identify essential messages to communicate to the public; learn best practices and innovations from other states; and use campaigns and incentives to raise public awareness. Communities need to know about evacuation routes, emergency shelters, and the basic parameters of their local community’s emergency response plans. Reinforcing earlier discussions about preparations, this document also calls on governors to ensure that the citizens in their state are prepared to be self-sufficient for at least 72 hours in the aftermath of a disaster, including maintaining an ample supply of food, water, and other necessities.

Overall, the research literature highlights three areas of recommendations for government leaders that are fairly applicable in any community setting worldwide:

1. Communicate effectively, provide accurate, truthful information before, during and after an incident.
2. Focus on influencing perceptions of competence, trust and good faith - before, during and after an incident - which can do a lot to reduce fear and panic; and
3. Set an example in what you communicate and how you communicate, because if you remain calm, others will follow your lead accordingly.

How individuals perceive their government’s prevention and emergency preparedness impacts on how they assess the threat of terrorism as well as their expectations as to how the government is most likely to respond in the event of a terrorist attack. Effective risk communication involves providing people with the facts they need to make best choices among the often-limited options available, being candid about what is known and the quality of the information being provided to the public. According to Durodie and Wessely, “One primary role is to fill the information vacuum before rumors, myths, misinformation, and ultimately hoaxes can take their course. Rapid, timely, clear, and repeated facts and data need to be at hand and presented by trusted sources, appropriate to relevant communities. Much of this can be prepared in advance but needs to be specific and robust rather than general or vague.” Further,

“The release of inaccurate, confusing, or contradictory information has the potential to increase levels of demoralization as well as discrediting the authorities concerned. Such failures of communication can create misunderstanding, suspicion, and resistance to future warnings that ultimately inhibit relief efforts.”

Unfortunately, as noted earlier, mass and social media can play a significantly negative role throughout manmade (and natural) disasters. Research from the fields of psychology, sociology, security studies and elsewhere have highlighted the unhelpful and irresponsible ways in which media often overemphasize portrayals of panicked behavior during disasters. Of course, because drama and fear attracts viewers and readers, a country’s profit-motivated...
media services have a business incentive to focus more heavily on the emotionally provocative aspects of an incident and downplay or ignore examples of calm, rational behavior among the victims.

But there should also be a recognition among the media that they have a responsibility in their reporting to help prevent - rather than exacerbate - the chances of panic in the wake of a terrorist attack. Similarly, governments must pay close attention to social media, which has been increasingly used by some ill-meaning individuals to spread rumors and disinformation, incite paranoia and hysteria, and reinforce prejudices and biases. Regrettably, certain prominent politicians have been known to engage in such negative behavior in order to gain some sort of political advantage.

Literature from the field of psychology describes how calm reassurances by government authorities in the wake of a terrorist incident can have a beneficial impact on anxiety levels among members of the public. The central goal of communication efforts during ongoing incidents and immediately thereafter should be to reduce fear while addressing misunderstandings and misinformation. In the wake of an incident, as Durodie and Wessely note, “The public can become victims of their fears - terrorizing themselves far better than terrorists can.” Government spokespersons should avoid emphasizing the vulnerabilities of the community, and instead focus on people’s resilience and provide specific, relevant information and recommended actions in a timely, authoritative manner. For example, after a series of four terrorist attacks in Germany within one week in July 2016, the spokesman for the Munich police made a public appeal: “Give us the chance to report facts. Don’t speculate, don’t copy from each other.” Most politicians and media services throughout the country heeded his advice. Only a small handful of fringe politicians - like the leader of the anti-immigrant Alternative for Germany (AFD) party - tried to capitalize on the attacks, and were immediately condemned on social and broadcast media. Similarly, after the 7 July 2005 terrorist attacks in London on the transport system, the Queen of England visited hospitals to meet victims and express sympathy. During a visit to the Royal London Hospital, she stated, “Those who perpetrate these brutal acts against innocent people should know that they will not change our way of life.” Finally, transparency and honesty are vital in such instances, in order to engender widespread trust in the government’s response efforts, and convey the message that by working together the society will make it through this. As the 2017 US National Security Strategy notes, “An informed and engaged citizenry is the fundamental requirement for a free and resilient nation.”

**Empowerment**

Finally, a third theme that is reflected in research - and in many emergency planning documents - highlights the central importance of partnerships, shared responsibility and empowerment. To be sure, citizens must be able to trust their government agencies and authorities responsible for safety and security. But it is commonly accepted that private citizens must also take some ownership for their own preparedness. This, in turn, requires a government to empower individuals to be proactive, give them a sense of purpose and direction in times of crisis, and provide ways for them to take responsibility for responding effectively when an incident does occur. Similar to preparedness, the central message in this area of strategic planning is to establish mechanisms through which individual members of society are provided opportunities to partner with government agencies in answering calls for help. Much of this empowerment has traditionally been organized at the volunteer level by non-profit and community organizations (e.g., the American Red Cross/Red Crescent). The public health sector will often organize blood donor drives, another way of empowering the members of a community to contribute towards an effective response to whatever crisis has emerged.
Meanwhile, governments have also sponsored various initiatives to empower their citizens. In the US, FEMA sponsors a Citizens Corps initiative that brings together government and community leaders to involve individuals in emergency preparedness and response. Participants in this program are asked to get training in first aid and emergency skills, become familiar with local emergency plans and resources, and to volunteer their assistance when called upon by emergency responders. Similarly, the Community Emergency Response Team (CERT) program educates volunteers about disaster preparedness for those hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, search and rescue, team organization, and disaster medical operations. Specific actions an individual could be empowered to do include providing food and clothing to survivors at relief shelters, assisting with search and rescue operations, directing traffic during evacuations, and many other kinds of tasks. By empowering local citizens to participate effectively in times of crisis, these programs also allow professional emergency responders to focus on more complex tasks. And to avoid redundancy or wasted efforts, tasks and responsibilities are to be coordinated by a comprehensive incident management plan and a command structure for emergency response.

Having a structure in place for community volunteers to get involved in response efforts is an essential form of empowerment. Few things have a greater impact on an individual’s perceptions and resilience than personal experience. Further, beyond empowering individual members of the public to be proactive in the face of terrorist threats, these types of efforts help create social bonding among community members, which also reduces panic in the wake of terrorist attacks. In fact, research has found evidence that the existence of such bonds among social groups may play a greater role in determining whether panic ensues than the response of the authorities themselves during an emergency. As Sheppard et al. note, “Military leaders’ perception that established units are less likely to panic under fire than newly formed units where members have yet to bond with each other also appears to hold weight in civilian life. The presence of familiar people can have a remarkably calming effect during an emergency, so much so that people will sometimes delay evacuating dangerous situations, or even enter dangerous situations, in order to maintain a personal bond with someone.”

In sum, there is extensive research on ways to prevent panic in the wake of terrorist incidents. Three prominent themes within this literature - preparation, communication and empowerment - offer useful guidance that governments should incorporate into their emergency response strategies. These strategies are known to bolster social trust, which is central to ensuring community resilience in times of crisis. And higher levels of community resilience lead to diminished likelihood of panic in the wake of terrorist incidents.

Research and Policy Implications

The culmination of these three areas of effort - preparation, communication and empowerment - is a more resilient community, one that can manage uncertainty more effectively. The policy implications of this research for governments and societies worldwide are fairly intuitive. The more a society commits itself to learning about and building community resilience, the more likely it will respond to any kind of emergency in a positive and constructive manner. Further, resilience can be a deterrent against terrorism: the more resilient a society proves to be in the face of a terrorist threat, the more likely the terrorists will recognize the futility of their efforts. Quite often, terrorist groups are opportunistic, using violence to take advantage of possible vulnerabilities in a society, in order to advance their political and ideological objectives. However, they will find no advantage and no success when the society they wish to weaken or disorient has invested in best practices of emergency preparation, communicates effectively, maintains trusted relationships between the government and the governed, and empowers community members with knowledge and tools to cope with any kind of terrorist attack.
However, as noted earlier, researchers have employed multiple definitions of “community resilience”, and definitional clarity is further complicated by variations in what we mean by “community” - a term that can include geographic, national, social, and economic boundaries, as well as cultural, ethnic, and racial dimensions. In general, a community is viewed as a collective group, one that often finds itself reliant upon others with whom they share something in common. In the face of adversity - which may include terrorism (or other forms of political violence and criminality), environmental hazards, and epidemics, as well as industrial accidents - communities must find ways to adapt as a collective group in order to remain viable and prosperous. For communities threatened or attacked by campaigns of political violence, the ability to retain positive cohesiveness is vital for a successful recovery.

While community resilience may be difficult to define, it is even more challenging to measure or to identify and implement effective strategies for improving it. Some scholars have suggested that resilience should be viewed as a multilevel construct derived from the capabilities of individuals and groups to sustain positive relationships, as well as endure and recover from stressors. Norris et al. equates resilience with the process of linking resources, referred to as adaptive capabilities, to outcomes, or adaptation. Expanding on Dohrenwend’s model of psychological stress (published in the late 1970s), Norris’ model examines various decision points and accounts for various resource factors whereby the community’s ability to adapt is a vital element for achieving resilience. Communities who are internally polarized, lack resources or are unable to adapt to challenges are vulnerable to persistent dysfunction. Accordingly, building resilience can be a positive process when it is linked to a network of adaptive capabilities after a disturbance: “to build collective resilience, communities must reduce risk and resource inequities, engage local people in mitigation, create organizational linkages...[and incorporate] flexibility, decision-making skills, and trusted sources of information that function in the face of unknowns.”

Ideas of self-efficacy are based upon the transfer of accountability to communities by building stronger societal pillars that can withstand shocks from man-made events such as terrorist incidents as well as natural disasters. Further, as described earlier, it is important to recognize that shoring up community resilience involves significant investments of effort before an incident occurs. It should be an ongoing process that is constantly addressing vulnerabilities and improving shortcomings, with a particular commitment to effective communication and public education. Various kinds of emergency preparedness efforts reduce doubt and uncertainty. These in turn increase the ability of a community to return to normalcy and diminish the potential for a terrorist incident to provoke panic. Further, resilience is built on foundations of trust, the strength of which can be increased by effectively communicating prompt and accurate information before, during, and after an event occurs. On the other hand, mistrust reduces the overall willingness of the community to become self-efficient and resilient. Government leaders must be committed to effectively communicating the risks of terrorism in a way that is comprehensible and inclusive to all sectors of the population, and to remain calm in the immediate aftermath of an incident.

There must also be a humble but honest acknowledgment that even though every measure is being taken to prevent a terrorist incident, it is unrealistic and irresponsible to encourage the expectation of 100% failsafe security. As noted earlier, risk perception is influenced by the amount of information individuals have about a potential incident, and people are more likely to feel that an activity or event is not dangerous if they are empowered to manage it (or control their response to it) effectively. Proactive measures before a terrorism event can thus set the tone for subsequent response behaviors. The goal is to provide the community with the ability to develop a calculated risk perception culture through a collaborative cycle of information sharing between subject matter experts and the public. Perceptions of credibility, objectivity, transparency and trust are essential here between the people producing information and those consuming it. Trusting the validity of information sources and the decision processes
involved in mitigating hazards enables people to become less afraid. In order to achieve a higher level of trust and develop a robust risk perception culture, officials need to improve information sharing, engage in efficient outreach programs, and increase public empowerment through involvement.

Perceptions of risk and community resilience also depend on trust in the local critical infrastructure. At a very basic level, this means having confidence that electric power and water supplies will remain available (or will be repaired very quickly), that the rule of law will be upheld throughout the community, and that the public health system is adequately prepared to function effectively in order to save as many lives as possible. Research has also found that community resilience is dependent on the development of healthy connections among individuals within that community. Positive, trusted relationships among a community’s members help ensure its collective efficacy and enhance their ability to adapt and recover from traumatic events. Thus, strengthening communal interconnectedness - what Daniel Aldrich describes as “communities’ social capital” - becomes central to increasing the ability to bounce back from major terrorist attacks or other unforeseen catastrophic events.

In politically polarized societies (as many Western democracies are today), this raises an important topic for further research: how to strengthen bonds of trust between government and civilians, and among civilians regardless of political affiliation, socio-demographic background, and so forth. A divided public fighting amongst themselves so bitterly is unlikely to come together effectively in times of crisis. The level of distrust and acrimony between and among members of “the public”, combined with diminishing confidence in government agencies and leaders, create a recipe in which the fear that terrorists seek to provoke can be amplified, thereby exacerbating the already daunting challenges of fostering community resilience. Government-led strategies and initiatives to build (or rebuild) social capital in polarized communities will necessitate the active engagement of the private sector, and religious and educational leaders.

Unfortunately, we do not yet have a clear understanding about what sorts of initiatives and programs exemplify best practices in building resilience. There is a fair amount of quality research (including case studies that identify best practices) on how to prepare for emergencies, communicate effectively, and empower citizens. But assessing these things before a terrorist incident occurs is another matter. How well-prepared is our community for an unforeseen crisis? How effectively do our leaders communicate in times of crisis? How empowered are our community’s members? Without accurate assessments of these things, there is no way to determine shortfalls or areas that need additional investment. Gaps in the research literature that need to be addressed also include finding methodologies how to accurately assess community resilience at specific points in time, in order to determine changes (positive or negative) and whether existing efforts to build resilience actually have a positive impact. What data should be collected and analyzed for this purpose? And further, how can those data help us evaluate whether any improvement over time can be properly attributed to certain programs or initiatives? If we are able to accurately provide evidence about which communities seem to be the most resilient, and why, the next area of research to be addressed involves determining whether strategies developed and applied in one context could be successfully transported for implementation in other contexts.

Similarly, more research is needed on how to assess (and then improve) the effectiveness of communication efforts, particularly in the modern era of social media-fueled disinformation. As noted earlier, when our perceptions of risk are misinformed and manipulated, this has a negative impact on our decision-making. Disinformation -regardless of its source - can reduce social trust and undermine efforts to build community resilience. Rumors, myths and hoaxes can spread all too easily via social media, so government authorities need to be equipped to rapidly respond by providing members of society with accurate facts and data. Failing to do so could increase levels of disorientation and demoralization among a community’s members,
and decrease their confidence in the government’s (and their own) ability to manage a crisis effectively. In a similar vein, the media have a tremendous responsibility to confront the spread of disinformation and help prevent - rather than exacerbate - the chances of panic outbreaks in the wake of a terrorist attack. Thus, policies and strategies are needed to ensure the media take this responsibility seriously, for the sake of community resilience.

Research-based public education programs are also needed for both emergency preparation and empowerment. As noted above, fear rarely produces panic or frozen shock, an inability to react at all. So, instead of implementing plans and policies based on inaccurate perceptions and expectations (fueled by the myth of panicked flight), government agencies should seek partnerships with community members, and ensure they are well-informed and equipped with the tools necessary to contribute productively to the management of a terrorist incident. Similarly, research in this area has identified issues that can reduce community resilience, and must be avoided. For example, new societal efforts are needed to curb the dramatization of terrorist incidents by the media, and to deter fear-mongering by politicians. Provoking fear on behalf of a political agenda has often involved directing people’s anxieties toward a specific “other” (immigrants, Muslims, Jews, homosexuals, etc.) in ways that are unjust, irresponsible and counterproductive. This, in turn, contributes to the kind of fear and polarization that undermines any effort to build social capital and strengthen community resilience. What is needed instead is a commitment to community preparedness, transparency, effective and transparent communication, citizen empowerment, and trust in each other. Together, these things strengthen community resilience in ways that can prevent public panic in the wake of a terrorist incident.

Conclusion

To sum up, evidence-based research has illuminated critical intersections between government preparedness, trust, transparency, effective communication, citizen empowerment and other efforts to strengthen community resilience. Policies and strategies based on solid research can benefit governments and communities worldwide. Unfortunately, there are widespread beliefs and assumptions about panic in the wake of a terrorist attack that are largely based on myth rather than fact. And when the media (and some politicians) encourage myth-making by envisioning a mass of panicked and passive victims in the wake of a terrorist attack, this leads to policies that are at best unhelpful, and potentially even counterproductive. But rather than encouraging fear (and even trying to capitalize on that fear for the sake of political agendas and profits), we must acknowledge the many things that individuals, families and communities can do - with and without their government’s involvement - to strengthen community resilience. Commitments and investments in these areas are bound to yield more sophisticated and successful measures to prevent public panic in the wake of a terrorist incident.

Juan Merizalde is a researcher and doctoral student in the School of Criminology and Justice Studies, University of Massachusetts, Lowell. His research interests include asymmetric warfare, the private defense sector, counter-terrorism policy, and community resilience. Previously, Juan served in the U.S. Air Force where he was deployed in Operation Enduring Freedom and Operation Iraqi Freedom.

John D. Colautti is a researcher and doctoral student in the School of Criminology and Justice Studies, University of Massachusetts, Lowell. He is also an Adjunct Professor at Fitchburg State University, an instructor with Crisis Systems Management, LLC, and an instructor with
the Massachusetts Municipal Police Training Committee. He has over 30 years of probation, law enforcement and private security experience.

James J.F. Forest is a Professor in the School of Criminology and Justice Studies at the University of Massachusetts Lowell. From 2010 to 2019 he was also a Senior Fellow at the U.S. Joint Special Operations University. Currently, he is a Visiting Professor at the Fletcher School of Law and Diplomacy, Tufts University. Previously, Dr. Forest was Director of Terrorism Studies at the United States Military Academy. During his tenure at West Point (2001-2010) he directed a series of research initiatives and education programs for the Combating Terrorism Center at West Point (CTC), covering topics such as terrorist recruitment, training, and organizational knowledge transfer. Dr. Forest also served as an Assistant Dean at West Point. Prof. Forest has published 20 books and dozens of scholarly research articles and reports in this field, and is co-editor of the peer-reviewed scholarly journal “Perspectives on Terrorism”.
Endnotes


2 Ibid., p. 2269.


6 Ibid.


9 Ibid., p. 90.


14 Butler, Panzer, and Goldfrank, 2003, p. 47; citing Human Rights Watch. ‘We Are Not the Enemy: Hate Crimes Against Arabs, Muslims, and Those Perceived to be Arab or Muslim...


22 Sheppard et al. 2006, p. 236.


26 Ibid., p. 88.


29 For more on this, see Forest, James J.F., *Digital Influence Warfare in the Age of Social Media* (Santa Barbara, CA: ABC-CLIO/Praeger, 2021).


39 DHS/FEMA Ready.gov website. Available at: https://www.ready.gov.


44 Sheppard et al. ,2006.

46 Ibid.
50 Ibid.
54 Sheppard et al. ,2006.
57 Norris et al.,2008.
58 Ibid., p. 145.
63 Khripunov, 2006; also, for a comparative study on the difficulties of educating the public before a terrorism event involving chemical weapons, see Sarah Hildebrand and Anthony Bleetman, ‘Comparative Study Illustrating Difficulties Educating the Public to Respond to Chemical Terrorism’. Prehospital and Disaster Medicine, 22(1), 2007, pp. 35–41.
Bibliography


Fischhoff, Baruch. ‘Communicating About the Risks of Terrorism (or Anything Else)’. American Psychologist, 66(6), 2011, pp. 520–531.


Hildebrand, Sarah and Anthony Bleetman, ‘Comparative Study Illustrating Difficulties Educating the Public to Respond to Chemical Terrorism’. Prehospital and Disaster Medicine, 22(1), 2007, pp. 35–41.


Web-based Resources

http://dx.doi.org/10.1080/18335330.2013.789594

Australia *National Strategy for Disaster Resilience*. Available at: https://bit.ly/2Q7LDYt

Fischhoff, Baruch (September 2011): ‘Communicating about the Risks of Terrorism (or anything else)’. *American Psychologist*, 66(6), pp. 520-531. Available at: https://www.cmu.edu/dietrich/sds/docs/fischhoff/AP%20Fischhoff.pdf


Jenkins, Brian M. and Bruce R. Butterworth, ‘Does ‘See Something, Say Something’ Work?’ Mineta Transportation Institute (December 2018). Available at: https://bit.ly/2Di6x49


US Department of Homeland Security, “Resolve to be Ready” Toolkit. Available at: https://www.ready.gov/NewYears

Chapter 32

Prevention of Major Economic Disruptions Following Acts of Terrorism — The Case of the 2002 and 2005 Bali Bombings

Richard J. Chasdi

The Bali I (2002) and Bali II (2005) bombings, conducted by Jema’ah Islamiya (JI) and its splinter group Al-Qaeda in the Malay Archipelago respectively, are watershed empirical case studies used to highlight the theoretical discussion about the economic consequences of terrorism with particular focus on the tourism industry and related services sectors. The analysis focuses on broader lessons learned, and relevant policy prescriptions for areas heavily reliant on the tourism industry that make use of public-private partnerships, both domestically and internationally. In terms of a theoretical discussion about economic consequences, discussion involves comparisons between three topics. First, damage caused by the Bali I and Bali II bombings and economic impacts nationally, regionally, and internationally, to comparable damage caused by 9/11 and certain natural catastrophes such as Hurricane Andrew and Hurricane Katrina. Second, tourism asset protection approaches from economic and legislative perspectives. Finally, police and military action approaches and disaster management programs. This analysis primarily makes use of the school of neo-realism’s “three level analysis” of conflict with its focus on explanatory factors and effects at and across three levels: the “international political system,” “nation-state,” and “individual.” To be more specific, the “international political system” explanatory factors include those that affected three or more states (e.g., the Global War on Terrorism (GWOT) and the SARS virus). The “nation-state” factors include regime type, level of modernization, and societal composition. Third, “individual factors” include individual leader personality and style of leadership characteristics, and small upper level elite group decision-making processes.

Keywords: Al-Qaeda in the Malay Archipelago, Bali bombings, counter-terrorism, economic consequences, Indonesia, Islamic extremism, Jema’ah Islamiya, prevention, terrorism, tourism.
The purpose of this chapter is to examine the prevention of major economic disruption following acts of terrorism, in particular acts of terrorism against the tourism industry. The Bali I and Bali II bombings will be used as case studies to extract lessons learned and develop relevant policy prescriptions for areas heavily reliant on tourism. The framework of discussion includes a concise literature review about the economic disruptiveness of terrorist acts, the emergence of JI and its allure, and a discussion about the ramifications of the Bali I and Bali II bombings.

For both the Bali I and Bali II bombings, economic effects, major Indonesian government responses, and lessons learned will be examined. In the case of lessons learned, discussion about the Bali I bombings revolves around prevention measures taken and not taken, and the political (administrative), financial, and legislative deficiencies revealed, and a description of business preparedness and consequence management.

An historical retrospective suggests terrorist assaults against tourist-related targets have comprised a relatively modest portion of a broader set of attacks. Alex Schmid highlights analysis of terrorist assaults against tourism-related targets, revealing that between 1970 and 2007, less than 1 percent of terrorist attacks in the Global Terrorism Database (GTD) targeted tourists. It is fair to say that rate is higher nowadays because as traditional government and military targets continue to be hardened, the value of attacks against “soft targets” has increased relative to the costs incurred to carry out attacks.

One useful measure to establish a baseline is comparing the economic impacts of the Bali I and Bali II bombings described below with the economic effects of the 1993 World Trade Center (WTC) bombing and the 9/11 events. In the case of the 1993 (WTC) bombing, the economic consequences of that event were very substantial, but primarily limited to WTC tower structural damage to power centers, “emergency systems,” and “smoke damage.” According to one New York Times report, the bomb exploded, “… causing hundreds of millions of dollars of damage ….” Plainly, this stands in stark contrast to the $22 billion USD in just insured losses caused by the 9/11 events.

**The Literature on Terrorism and Tourism**

This brief literature review describes the “terrorism-tourism literature” with attention to economic security preparations relevant to pre-Bali I and pre-Bali II bombing conditions. The literature is broken down into three categories:

1. Assessment of broader 9/11 economic effects to compare economic impacts to the Bali I and Bali II bombings.
2. Approaches regarding tourism and related asset protection primarily from economic policy and legislative perspectives.
3. Examination of police and military actions and the role of disaster management programs that, inter alia, help to protect economic assets more completely.

In the case of literature that allows for comparison between the economic impact caused by the Bali I and Bali II bombings and 9/11, Etti Baranoff describes the economic impact of 9/11 on the American insurance industry. He compares 9/11 economic damage rates to natural disasters such as Hurricane Katrina (2005) and Hurricane Andrew (1992). Those two natural disasters caused the two highest rates of economic damage that the American insurance industry had to contend with, followed by 9/11: Hurricane Katrina caused roughly $69 billion in insured losses, in contrast to Hurricane Andrew, with circa $24 billion in insured losses. The damage caused by the 9/11 events ranked a very close third with insured losses valued at, as previously mentioned, $22 billion.
While attacks against tourism targets remain limited in scope, tourist arrivals worldwide were approximately 916.3 million in 2008, dropping some 4 percent to 800 million a year later.\footnote{While attacks against tourism targets remain limited in scope, tourist arrivals worldwide were approximately 916.3 million in 2008, dropping some 4 percent to 800 million a year later.}

In the narrower sense, for US tourism, losses as a function of 9/11 from 2000-2007 were substantial. Fall and Epkins cite US Department of Commerce statistics and report that if tourist arrivals by Mexican and Canadians tourists are excluded from the tally, “… overseas travel to America has declined 8 percent since 2000. In 2000, the United States welcomed almost 26 million overseas visitors. Seven years later, the United States welcomed 24 million overseas visitors.”\footnote{In the narrower sense, for US tourism, losses as a function of 9/11 from 2000-2007 were substantial. Fall and Epkins cite US Department of Commerce statistics and report that if tourist arrivals by Mexican and Canadians tourists are excluded from the tally, “… overseas travel to America has declined 8 percent since 2000. In 2000, the United States welcomed almost 26 million overseas visitors. Seven years later, the United States welcomed 24 million overseas visitors.”}
The authors appraise the financial loss incurred as a direct result of 9/11, and as a function of related factors that contributed to a downturn in tourist arrivals to the US. Those factors include, but are not limited to, hostile tourist environments that resulted from American fears and suspicion, and the ongoing Global War on Terrorism (GWOT).

Studies that focus on tourism and related asset protection from economic and legal points of view include: Bandyopadhyay, Sandler, and Younas (2014); Ghaderi, Saboori, and Khoshkam (2017); Lakdawalla and Zanjani (2002).

Bandyopadhyay, Sandler, and Younas distinguish between “transnational” and “domestic” terrorist attacks to compare how “transnational” assaults and “domestic” assaults affect levels of Foreign Direct Investment (FDI) as measured in the relation to a country’s GDP. They examined “… the percentage of net FDI inflows to GDP (FDI/GDP) taken from World Development indicators.”\footnote{Bandyopadhyay, Sandler, and Younas distinguish between “transnational” and “domestic” terrorist attacks to compare how “transnational” assaults and “domestic” assaults affect levels of Foreign Direct Investment (FDI) as measured in the relation to a country’s GDP. They examined “… the percentage of net FDI inflows to GDP (FDI/GDP) taken from World Development indicators.”}

Bandyopadhyay et al. conclude that “at the margin”, without taking into account domestic terrorism’s higher frequency that tends to equalize effects, one discrete event of “transnational” terrorism has more of a negative effect on FDI/GDP than one discrete event of “domestic” terrorism.\footnote{Bandyopadhyay et al. conclude that “at the margin”, without taking into account domestic terrorism’s higher frequency that tends to equalize effects, one discrete event of “transnational” terrorism has more of a negative effect on FDI/GDP than one discrete event of “domestic” terrorism.}
The primary reason for this is that transnational terrorists, with their infrastructure and resources located primarily in a foreign country, are not very vulnerable to local counterterrorism efforts. In addition, the authors find “aggregate aid” is particularly adept at reduction of domestic terrorist effects on FDI. In subsequent analysis that breaks down “aggregate aid” into “bilateral” and “multilateral” assistance, “bilateral aid” is found to be more effective in combating “transnational” terrorism’s ability to reduce FDI/GDP, while “multilateral aid is more effective vis à vis “domestic” terrorism.”\footnote{The primary reason for this is that transnational terrorists, with their infrastructure and resources located primarily in a foreign country, are not very vulnerable to local counterterrorism efforts. In addition, the authors find “aggregate aid” is particularly adept at reduction of domestic terrorist effects on FDI. In subsequent analysis that breaks down “aggregate aid” into “bilateral” and “multilateral” assistance, “bilateral aid” is found to be more effective in combating “transnational” terrorism’s ability to reduce FDI/GDP, while “multilateral aid is more effective vis à vis “domestic” terrorism.”}

A 2017 study by Ghaderi, Saboori, and Khoshkam examines the relationships between tourist arrivals and several independent explanatory variables that include security, exchange rate, travel cost, tourism infrastructure (i.e., hotels, room availability), and GDP. In the case of the independent variable security, the authors create an aggregate security indicator composed of “political,” “economic,” and “social security” components that is regressed onto the dependent variable, “tourist arrivals” (along with the other variables mentioned), with interesting results.\footnote{A 2017 study by Ghaderi, Saboori, and Khoshkam examines the relationships between tourist arrivals and several independent explanatory variables that include security, exchange rate, travel cost, tourism infrastructure (i.e., hotels, room availability), and GDP. In the case of the independent variable security, the authors create an aggregate security indicator composed of “political,” “economic,” and “social security” components that is regressed onto the dependent variable, “tourist arrivals” (along with the other variables mentioned), with interesting results.}

The authors find that in the case of developed states, there is a positive relationship between the aggregate security variable and tourist arrivals, where a one-unit level increase in total security results in an uptick of 1.3 percent for tourist arrivals. In contrast, for developing states, there is an inverse relationship, where a one-unit level increase in total security leads to a 4.1 percent decrease in tourist arrivals. This could perhaps be due to tourist perceptions of unsafe travel conditions in developing states as reflected in government efforts to enhance security. The analysis concludes that a high level of security while crucial to tourist arrivals might not be as significant for tourist arrivals in developing countries as are the independent variables, “tourism infrastructure” and “GDP.”\footnote{The authors find that in the case of developed states, there is a positive relationship between the aggregate security variable and tourist arrivals, where a one-unit level increase in total security results in an uptick of 1.3 percent for tourist arrivals. In contrast, for developing states, there is an inverse relationship, where a one-unit level increase in total security leads to a 4.1 percent decrease in tourist arrivals. This could perhaps be due to tourist perceptions of unsafe travel conditions in developing states as reflected in government efforts to enhance security. The analysis concludes that a high level of security while crucial to tourist arrivals might not be as significant for tourist arrivals in developing countries as are the independent variables, “tourism infrastructure” and “GDP.”}

Lakdawalla and Zanjani’s work, with its focus on the effects of government support for anti-terrorism insurance programs, is an example of an economic policy approach to counterterrorism. The authors examine whether government-supported insurance programs work to ameliorate a skewed condition where different levels of protection exist, as firm owners either decide to augment private security on their own (or not), and instead rely on
public provisions - namely law enforcement. The central notion is that terrorists, as rational actors, will tend to target “soft” unprotected firms, whose owners are unable or unwilling to take advantage of private “self-protection” measures. Hence, “… each target’s probability of attack falls with its own self-protection, but rises with the self-protection investments of others.”

The authors point out that firm owners, when making counterterrorism “self-protection” decisions, do not take the needs of others into account. The crux of the argument is that it is difficult for government to tax private “self-protection”, and thus to take into account free rider problems with firms in close proximity to “self-protection” firms that benefit from those private protection efforts because security in immediate proximities is an indivisible commodity.

Hence, if protection level differences between targets cannot be equalized through taxation, the option is to focus on insurance subsidies. The authors report that for this to work, “self-protection” and insurance protections must be equally effective, working in a condition where each firm pursues its own self-interest, knowing others will do the same. In this so-called Nash equilibrium condition, no firm deviates from pursuit of self-interest, (e.g., collusion with others to acquire a benefit), provided others do not. In the case of the Bali bombings, the issue of government sponsored insurance programs, their feasibility, and under what circumstances, is broached in this chapter, and in the broader sense by authors cited in this literature review.

Lastly, in the case of work that focuses on police and military security involvement and creation of disaster management programs, examples of work that explore effectiveness and feasibility issues include: Asongu and Nwachukwu (2018), Gurtner (2016), and Metodijeski and Filiposki (2016).

Asongu and Nwachukwu focus on factors internal to a country with a comparative analysis of firstly, law enforcement and private security, and, secondly, “armed services personnel” effectiveness. The aim is to shed light on the capabilities of each type of security apparatus to reduce negative externalities caused by terrorism on international tourism, as measured by “tourist arrivals.” In their analysis, the authors focus on four factors or measures of terrorism intensity called “policy syndromes” to assess comparative effectiveness. Those include numbers of deaths, numbers of injuries, property damage, and terrorist incident frequency. The scope of the study includes 163 countries for the period 2010-2015.

The authors generate results that suggest that “armed services personnel” are critical in efforts to reduce terrorism’s negative effects in three out of four “policy syndromes” — property damage, injuries, and incident frequency. The findings for law enforcement and other security personnel were not found to be statistically significant, leading to the conclusion that law enforcement and other security “… are necessary but not sufficient to mitigate the adverse consequences of terrorism.” Those results may be particularly important for Indonesia and Bali, as Thompson (2011) notes that “a 1% increase in terrorism attacks decreases tourist arrivals per capita by 0.07% in developed countries and by 0.38% in developing countries.”

Instead of focusing on military and police response efficiencies, Gurtner, in her work on Bali, focuses on the need to develop “disaster risk management” regimes with anticipatory governance and foresight emphasis. Those “disaster risk management” systems put a premium on an integrated set of pre-attack preparations to reduce risk, with an eye to promoting sustainable economic development at every stage of the emergency preparedness process.

What seems significant here is the concept of risk insofar as risk, according to Monahan, can be assessed in two basic ways. For Monahan, risk can be conceptualized in an actuarial sense, as the likelihood or probability of victimization, or risk can be analyzed as “risk abatement,” namely the removal or reduction of explanatory factors and their harmful effects. Gurtner appears to embrace the notion of “risk abatement” (also applied in this chapter on Bali case studies), where local communities must be integrated more effectively into governmental risk preparedness plans, perhaps with political and economic incentives, produced since the Bali I and Bali II bombings.
For Gurtner, one aspect of sustainable development is diversification of local economies where, in the case of Bali, there has been some effort at modification of the tourist industry to promote more specialized tourist options, what she calls “boutique” options, which cater to travelers that are more affluent. A critical part of Gurtner’s discussion involves corporate social responsibility (CSR) measures taken as part of “disaster management” by larger firms in tourism and related industries to provide worker education, retraining programs, and enhanced resilience. Gurtner argues that CSR initiatives would provide workers with the educational and economic wherewithal to adjust to fabricated economic shocks to local economies such as terrorism, or natural disasters such as tsunamis.21

In ways that echo the aforementioned, work by Metodijeski and Filiposki describes the importance of an integrative approach to “crisis management” preparation. Thereby emphasis is placed on inclusion of three components:

1. National counterterrorism stratagems and “training programs.”
2. Marketing through advertising campaigns.
3. Broader integrative tactical preparations for various stakeholders in the security system such as hotel industry personnel, the police, and military.

Metodijeski and Filiposki, who draw on the work of Paraskevas and Arendell, describe a five-fold sequence of “anti-terrorism policy” development with stages that include work to craft a “proficient anti-terrorist group,” intelligence/analytical divisions, set of protocols for formulation and implementation plans, and a series of monitor and oversight function programs that scope out clear issue and functional areas of responsibility.22 For both Gurtner and Metodijeski, and Filiposki, emphasis is placed on more integrative, holistic conceptions of the terrorism threat and the counterterrorism response to introduce flexibility into the system to make it more effective and efficient.

Jema’ah Islamiya — Growth and Allure

The Bali bombings were the work of Jema’ah Islamiya (JI). JI is a splinter group of Darul Islam (DI), an Indonesian Islamic extremist organization that emerged in 1942. Nugroho points to three themes that characterize the “Indonesian Islamic terrorism” discourse, ranging from Darul Islam, crafted by Raden Sekarmadji Maridjan Kartosoewirjo, to JI. For Nugroho, those three themes include the notion of defensive Jihad (jihad difai), a binary conceptualization of the world into believers and non-believers, and conspiratorial points of view about world domination “... under Jewish and Western civilization to destroy Islam.”23

JI was formally crafted in 1992 by Abdullah Sungkar who had a personal rivalry and disagreement with DI chieftain Ajengan Masduki about Masduki’s piety. Estimates about the size of the JI cadre vary: while Nugroho, for example, reports some four hundred activists comprised the JI cadre through 2012, Chalk and Ungerer report a much larger number of some two thousand activists.24 A set of “nation-state” factor effects, and what neo-realisits call “international system” level factor effects, coalesced to make it possible for Abdullah Sungkar and Abu Bakr Ba’aysir to grow membership in JI and thicken its ties to Al-Qaeda in Afghanistan and in Pakistan.25

Indonesia under Suharto (1966-1998) was a “fierce state,” to use Ayubi’s term, where the state predominated over society in the absence of a social compact; where clientelism, coercive behavior, and an enhanced security apparatus, induced compliance.26 At the “nation-state” level, President Suharto’s manipulation of non-violent Islamic organizations was a crucial factor where, in efforts to retain political control, Suharto loosened restrictions against non-violent Islamic organizations in efforts to build political alliances for his own political survival. A basic mistake made by the Suharto government that led to long-haul security problems for Indonesia was insufficient recognition of, or indifference to, the links between those non-
violent Islamic organizations and violent Islamist extremists and the permeability between those types of organizations.27

A second “nation-state” level factor whose effects accelerated the growth of Islamist extremism was Suharto’s 1998 resignation. The fall of Suharto’s “New Order” revolved around economic pressures caused by the Asian economic crisis (1997-1998). By itself this was an “international system” level factor, and an outcome of the political pressures associated with Suharto’s repression of political enemies and his indifference to the plight of most Indonesians. Thus, Rabasa reports that “Suharto’s downfall, to a large extent a consequence of the economic crisis, sharpened competition among the political sectors, some of which saw Islam as a path to political power.”28 At a functional level, with the end of the Suharto era, the organizational separation of Indonesia’s military into its national army, the Tentara Nasional Indonesia (TNI), and into POLRI, its national police force, also provided room for Islamic extremism to grow and thrive as administrative protocol, areas of responsibility, and communications capacities were still in their formative phases.29

Suharto’s resignation, followed by efforts to establish a more democratic political system in Indonesia, and the relative political tolerance that ensued, created opportunities for Islamic extremism to expand while links between local militias and non-violent Muslim political parties and movements continued to grow. At the same time, at least some of that newly found political tolerance in Indonesia was a result of government functional problems, namely problems with the capacities of early post-Suharto governments to project power in areas more distant from Jakarta.30 The problems those early post-Suharto governments had projecting power into the hinterland worked to the advantage of terrorist groups. For example, in the case of the Bali I bombings, at least some of the bomb materials for the attack used, namely the TNT involved, was transported from Ambon (Maluku) to Bali on widely used roads, apparently without fear of interception by Indonesian security forces.31

An important consequence of Suharto’s resignation was its effect on the Indonesian military. The Indonesian military, jockeying for political position in post-Suharto Indonesia, actually mirrored President Suharto’s tactics by working to curry favor with Islamic extremists for political advantage.32 For some Indonesian citizens it was frequently the economic hardships associated with the Asian economic crisis, the predominant macro-economic international system level factor in play at that time, that intensified the allure of Islamic extremism as a political alternative to government-supported Islamic political institutions such as Nahdlatul Ulama and Muhammadiya.33 While Suharto’s short-sighted efforts to court Islamic organizations, irrespective of their actual composition was a tragedy — an avoidable mistake but understandable, perhaps even predictable, given Suharto’s acute desire to retain power — the Asian economic crisis and its effects on populations comparatively new to city life, as well those in the Indonesian countryside, were beyond the control of Indonesia’s leadership.

Another “nation-state” level factor that influenced the growth of JI was the condition of local communal conflict in Indonesia, primarily between Muslims and Christians. This communal conflict happened in cities such as Poso (Sulawesi), Ambon (Maluku), and Sampit (West Kalimantaen), and exacerbated tensions between Indonesian Muslims and Christians, where in Poso, North Maluku, and Maluku, Christians also murdered Muslims. One crucial effect of this condition was that it diverted the attention of the Indonesian National Police (POLRI) away from the increasing threat of domestic Islamic extremism in Indonesia.34

What also contributed to JI’s growth was its actual involvement in the communal conflicts in Ambon, Maluku, and Poso. In Poso, for example, local Muslims, in exchange for protection against Christian militias, provided safe-haven to JI activists.35 In Maluku, JI activists, primarily from “Mantiqi I,” JI’s organizational division for Singapore, southern Thailand, Malaysia, and Islamic extremists from others groups such as Darul Islam (DI), fought together under the banner of an organization known as Laskar Mujahideen.36
Separatist movement activity in Indonesia, with its imputed economic costs in terms of what the military had to spend to constrain it, was a further “nation-state” level factor that contributed to the growth of JI and other Islamic extremist organizations. Separatist movements were operative in East Timor (1999), in Aceh with the Free Aceh Movement (GAM), and in West Papua with the Free Papua Organization (OPM) where significant threats of violence from such paramilitaries did not pass into eclipse until 2002, and in some cases lasted until 2005.37

Turning to the “international system” level, the effects of the Global War on Terrorism (GWOT), the dominant macro-political “international systems” level factor at work, interacted with communal conflict and separatism at the “nation-state” level to inhibit the Megawati government from making a more complete commitment to combating the growth of Islamic terrorism. Prior to the Bali I bombings, part of the problem was government denial that a significant threat from Islamic terrorism existed internally, a problem that appears to have been related to its preoccupation with communal conflicts and separatist movements.

A related factor responsible for the Indonesian government’s inability to commit itself more fully to the Global War on Terrorism was a carefully reasoned political appraisal by Indonesian political leaders about the prevailing opinion among Indonesians regarding American counterterrorism actions. The conventional wisdom held by many Indonesians was that GWOT illuminated a post-9/11 American plot to prosecute a global war against Islam. Such conspiratorial anti-American sentiments were even found among members of political families at the highest level of Indonesia’s government. For example, President Megawati’s “own sister...Rachmawati Soekarnoputri...dismissed reports of radicalism within Indonesia as CIA ‘rumours’ designed to undermine Islam and put Indonesia under US control.”38

Hence, President Megawati, as a rational actor, appears to have conducted a cost-benefit analysis — the costs of political blowback portraying her as an American stooge, willing to use “hardline” Suharto-like actions, was more costly and difficult for her to bear than reaping the benefits of a more robust response to the threat of Indonesian Islamic extremism. Within the context of the transition from Suharto to a more democratic leadership where Indonesia’s weak governments were trying to establish legitimacy, public opinion and perception certainly mattered.39 While the Suharto resignation remains a critical factor for the rise of JI and other Islamic extremist organizations, the weakened condition of early post-Suharto governments with their legitimacy and power projection problems seems equally important. This then, was the background to the Bali bombings.

The Bali I Bombings (2002)

The Bali bombings of 12 October 2002 were carried out by JI against two sites in Kuta, Bali’s popular tourism locale, and at a third site in Sanur, close to the US consulate. Those terrorist assaults caused the deaths of 202 persons and injuries to up to 500 others. Both sites in Kuta were frequented regularly by regional tourists from countries such as Australia and Japan, and tourists from Western countries such as the US, UK, Ireland, and Germany.40

The most devastating detonations took place in Kuta at the Sari Club discotheque and at Paddy’s Bar where the curbside potassium chlorate explosive devices used were packed into a plastic file cabinet inside a parked Japanese minivan, at least in the case of the Sari Club. The IED near the front of the Sari Club was considerably more powerful than the device used at Paddy’s Bar, but it was at Paddy’s Bar that suicide bomber “Jimmy” entered the premises, marking a departure from past JI events.41 Those high intensity assaults are consistent with Baker’s broader observation that, “...most of the JI bombings attacks since 2004 have involved multiple or large bombs aimed at indiscriminately producing substantial numbers of casualties.”42
Bali as a Target

Why target Bali? Ostensibly, the long-term objective of JI at that time was to cull out an “Indonesian Islamic state” (Da’ulah Islamiya) as a springboard to create a broader regional Islamic polity in Southeast Asia. However, for Balbi, intertwined political and religious motivations tracing an arc to Indonesian religious conflict in the 1940s are more nuanced sources of both of the Bali bombings. Those attacks also reflected a visceral response to increased socio-economic development and the new emphasis on democratic reform. Balbi quotes Lewis and Lewis, who asserted that “the relationship between Bali and Java represents the complex modernization of Indonesia and the “constitutional fabric of Indonesia’s democratic statehood”, and in this sense, the Islamic militant terror attacks were also an assault on the “very essence of the Indonesian state and its politico-cultural integrity.”

For Hitchcock and Darma Putra, “opportunity recognition” and international political factors made Bali a high-profile targeting opportunity, where an attack would command extensive media coverage. There was symbolic importance to high intensity attacks in the post-9/11 world against Westerners, particularly Americans and Australians in this case, because the Australian government had, in the 1990s, provided close cooperation to the Clinton administration as it confronted the Indonesian political leadership’s response to East Timorese self-determination efforts with brutal Indonesian military repression.

The anticipated role of media related to the attacks did not go unnoticed by JI chieftains. The benefits of extensive media coverage of Bali I promoted the political message of confrontation with the West over the GWOT. It also highlights what Hudson describes as the GWOT’s heavy emphasis on military actions and “regime change.” That message dovetailed well with JI and al-Qaeda’s economic motivations to damage the world economy. Media coverage of the Bali bombing could create fear among tourists and help cripple the Indonesian economy and Bali’s tourism industry.

At the same time, the vast religious, ethnic, and cultural differences between JI perpetrators and Bali’s Hindu community made Bali, with what Balbi calls its “secularism,” an even more attractive terrorist target, as the Balinese who are Hindu stood out in sharp religious contrast to Java’s majority Muslim population. Within the context of those religious and social cleavages, Balinese were seen by Islamic extremists as somehow complicit in post-9/11 American counterterrorism operations.

The choice of Bali as a target was also influenced by JI’s close ties to Al-Qaeda. JI’s own origins trace an arc to contacts in the early 1990’s between Osama bin Laden and JI founder Abdullah Sungkar. According to Nugroho, “their linkage to Al-Qaeda is the result of the identical ideological bondage of global Salafist doctrine envisaged to create a caliphate in Southeast Asia.”

For Islamic extremists, Westerners have a high degree of symbolic importance as targets within an imagined fierce eschatological struggle between the West and Islam; they are viewed by Islamic extremists as legitimate targets because they live in “ignorance” or darkness (jahaliya), in Dar al-Harb (“the house of war”), or outside the enlightened community of believers, the Muslim ummah. In the middle to late 1980s, Sungkar and Abu Bakr Ba’asyir, who were both living in exile in Malaysia since 1985, established networks with Al-Qaeda and a Southeast Asian recruit pipeline of activists to fight in Afghanistan, before their return to Indonesia in 1998.

The Bali I Operation

It was JI member Imam Samudra who hatched the plan to assault Bali, but Mukhlas (aka Ali Gufron), who worked with JI chieftain Hambali (aka Riduan Isamuddin), appears to have been in charge of the actual operation. The JI group involved in the Bali bombings was divided
into two units: one responsible for target surveillance and a second group to carry out the operation. JI’s capacity to engage in target surveillance was ample. For Baker, the focus of “...JI bombing operations to date has been an emphasis on extensive target identification and surveillance.”53 Syahfullah, a Yemeni who was an Al-Qaeda activist, worked with Mukhlas and Imam Samudra on administrative and logistics issues, while the Malaysian JI reconnaissance expert Zubair helped to identify specific targets.54 The major Bali I perpetrators were middle-to-high-echelon JI activists with overlapping affiliations with other terrorist organizations that were operating internationally. Those included JI chieftain Zulkarnaen (aka Aris Sumarsono or “Daud”), the Indonesian senior “JI operations chief,” bomb maker, and interlocutor between al-Qaeda and JI, who would also go on to collaborate with Noordin Mohammad Top to carry out the Bali II bombings (2005). Fathur Rahman al-Ghozi, was another main JI actor who trained JI recruits in Mindanao and served as JI interlocutor to the Moro Islamic Liberation Front (MNLF).55

Several scholars such as Nugroho point to the importance of the war in Afghanistan, where many JI chieftains gained military experience to pass on to Southeast Asian Islamic extremists, as crucial to the enhancement of JI effectiveness. Further, those international connections established in training camps in places like Afghanistan, Pakistan, and the Philippines, made it possible for Jihadists who knew one another to establish networks for future collaborative efforts.56 It is well known that networks are the transmission mechanisms of social movements. They cause “social mobilization” in individuals and small groups of individuals that, in turn, can lead to structural political change.57

The JI group was also comprised of several others including three brothers: Amrozi bin H. Nurhasyim who was a motorcycle repairman, Ali Imron, as well as Mukhlas.58 Dr. Azhari bin Husin, an engineer by training and considered the senior bomb-making specialist in this group, crafted the bombs, while his student Dulmatin (aka Joko Pitono), a capable bomb-making and electronics specialist in his own right, presumably worked with him. In addition, Idris (aka Joni Heidrawan), an Indonesian who detonated the US consulate device, presumably worked with Umar Patek (aka Abdul Ghoji), who was another Indonesian bomb maker.59

What is significant here is the permeability of many terrorist groups, personnel, and the thickness of family connections (e.g., the brother-in-law of Dulmatin, Hari Kuncoro, was also a conspirator). Those findings about JI composition dovetail well with previous findings of this author about the importance of family and personal connections between activists of al-Ittihad al Islamiya (AIAI), the al-Qaeda affiliate responsible for the Mombasa and Kikambala terrorist assaults against Israeli targets in November 2002.60 It should be noted that both Rabasa and Hitchcock and Darma Putra suggest Abu Bakr Ba’asyir might not have supported the Bali bombings outright because he believed that JI’s commission of frequent terrorist assaults would elicit the special focus of the Indonesian police and counterterrorism measures onto JI.61

The Bali bombings display the rationality assumption in decision-making where terrorist chieftains are considered rational actors who engage in cost-benefit analysis within the context of “opportunity recognition” for target selection. By contrast to the enormous economic damage caused by the Bali I bombings to Bali’s local economy and the substantial damage to the national economy described below, Hastings asserts that JI chieftain Mukhlas had only some $30,500 supplied by Al-Qaeda to spend on the Bali bombings.62 Plainly, terrorist leaders understand how economic cascade effects from carefully planned terrorist attacks can disrupt national economic development plans.63

As a rational strategy, focus on tourism target venues, especially in the post-9/11 era, appears to be pronounced with attacks in places as varied as Indonesia, Morocco, Sri Lanka, India, Egypt, Fiji, and Mali.64 In the case of the Bali I bombings, Gurtner, Rabasa, and Henderson all suggest that early warning systems (EWS) and other prevention or disruption instruments and protocols were virtually non-existent in the pre-Bali bombing period. For Henderson, this extended into the realm of strategic assessment. As she reported, “regarding
strategy ingredients, there is no evidence of formal attempts to identify threats or devise plans prior to the attack.”

Rabasa points out that “Indonesia…had just emerged from authoritarian rule and lacked the equivalent of an Internal Security Act that would allow the authorities greater latitude in dealing with suspected terrorists.” Likewise, Gurtner concludes that after the Bali I incidents, while “safety and security measures with related education and training had improved, however Bali still lacked a formal disaster management plan.” Indeed, a statement made by Indonesia’s future president right after the Bali I attacks is very telling with respect to what were security priorities. As reported by The Guardian, “security minister Susilo Bambang Yudhyono said strategic targets, such as liquefied natural gas plants, ‘will be protected.’”

Some accounts suggest that the economic effects of the Bali I bombings were compounded by broader macro-economic factors such as the Asian economic crisis. However, it remains unclear just how or to what degree the Asian economic crisis or other exogenous events such as the SARS virus epidemic exacerbated the effects of the Bali I bombings on Indonesia’s national economy. That uncertainty resonates with Drennan’s point about the inherent difficulties of sorting out broader terrorist incident effects from the effects of other confounding conditions such as the post-1998 regional recession.

**Economic Effects of Bali I**

In the broadest sense, Schmid reports that the world tourist arrival rates, dropped 25 percent in 2003 after the Bali bombings of October 2002. Some of the economic effects of the Bali I bombings could be captured by incremental weekly or monthly data about hotel occupancy, for example, sorted out into broader effects on the Indonesian national economy and more localized economic effects in Bali that involved the Balinese hotel management industry, hotel workers, vendors, and subcontractors. However, such detailed data are not available.

Henderson captures the magnitude of financial loss in the aftermath of the Bali attacks, noting that “the Tourism Ministry speculated about losses of $1.8 and $2 billion from international and domestic tourism earnings respectively, equivalent to about 6.6% of the country’s GDP, leaving 2.7 million unemployed….” Balbi points out that the disruption of Bali worker remittances to families in parts of Java after the Bali I bombings also had substantial economic effects that contributed to the damage inflicted on Indonesia’s national economy. Further, there were other broad economic effects such as a decline in Indonesia’s reserves of foreign currency and decline in incoming foreign investment.

The Bali I terrorist assaults had the most profound economic repercussions locally. As 90 percent of Bali’s revenues were, at the time, tourism driven, the downturn in tourism to Bali increased unemployment among the ranks of local workers such as small merchants and taxi cab drivers associated with the hotel and tourism industries, and hence contributed to a decline in the income that local families earned. One World Bank estimate is that on average, there was a 40 percent decline in income from November 2002-May 2003. Hitchcock and Darma Putra reported that “tourist arrivals” dipped considerably in the months following the Bali I terrorist assaults.

Thus, in September 2002, there were 150,747 tourist arrivals in Bali, a number that continued to dip over a three-month period to 60,836 by January 2003. That represents a 40.35 percent reduction in tourist arrivals from 150,747 in three months. In February 2003, “tourist arrivals” increased by 6,633 and steadily grew through March 2003 to 72,263 people. From that time until August 2004, when tourist arrivals reached 155,628, tourist arrival rates per month were marked by cyclical patterns, with a range of between 47,858 to 148,117. The last figure represents about 98.2 percent of the volume listed for September 2002. Compared to the American tourist rate dip of some 8 percent over seven years from 2000-2007 following 9/11,
these indicators appear to reflect much greater volatility in the case of the Bali experience, perhaps in part because of Bali’s small size and lack of economic diversity beyond tourism.\(^{77}\)

In a similar vein, accounts in *The Straits Times* also point to the potency of the short-run effects of those attacks: in the week after the 12 October 2002, Bali I terrorist assaults, “hotel occupancy” in Bali diminished by some 44.6 percent, from 74.8 percent to 33.4 percent hotel capacity, from 11 October 2002, to October 2019, amidst the combined effects of abject fear and foreign government issued travel warnings and advisories. Indeed, both Henderson and Hitchcock, and Darma Putra reported that by late October 2002, Bali’s hotel occupancy rates had in some cases as in Nusa Dua, diminished to some 10.0 percent.\(^{78}\) To provide some middle-range perspective to this, Schmid reports, “after 9/11, both airline passenger loads and hotel occupancy in the United States declined for several months by 50% and more in some regions.”\(^{79}\)

There were also Southeast Asian regional and international effects — Malaysia for example, suffered a smaller downturn in “tourist arrivals,” about two-thirds of the drop in Bali’s “hotel occupancy” as reported by Asmarani; tourist arrivals for October 2002 plummeted “…28 percent to just over one million, compared to a forecast of 1.4 million.”\(^{80}\) However, Bali’s tourism rate experienced again an uptick due to, at least in part, interregional tourism from places such as Japan, Singapore, and Australia. Hitchcock and Darma Putra noted that “by 2004 the situation had improved markedly with foreign arrivals returning — and in some cases exceeding (see January 2004) — the pre-bombing record…” as measured per month, primarily by the Bali Tourism Authority.\(^{81}\)

In the case of the “Typology of Terrorism’s Economic Disruptions” presented in Appendix I, the Bali I attacks appear to fit most closely with type ten, (A1 B4 C1) where “economic disruption effects of a terrorist assault against a tourist target (have) international effects and national effect and/or regional effects in a short-run interval” (See Appendix I).

**Indonesian Government Economic Responses to Bali I**

The purpose of this section is to explore briefly some of the Indonesian government’s more important economic responses to the Bali I bombings. International assistance efforts to Indonesia and to Bali, in particular after the Bali I bombings, are well documented with multilateral assistance provided from institutions that include, but are not limited to, the World Bank and the United Nations (UN Development Program). As Lewis reports, “donor and development organizations such as USAID, the World Bank, Dutch Trust and AusAID have also developed a range of social and infrastructure programs, mostly focused on the restoration of tourism.”\(^{82}\)

The Indonesian government also implemented some carefully reasoned policies of its own in both economic and political/cultural domains — with mixed results. In efforts to promote societal resilience and economic recovery nearly simultaneously, the Indonesian national government, with involvement of provincial and district governments, focused its efforts primarily on economic recovery.\(^{83}\) Those efforts included, but were not limited to, about $ 4 million, with an additional $ 1 to 2 million more specifically geared towards tourism, infused into Bali (e.g. through the Bali Tourism Authority) by Indonesia’s national government.\(^{84}\)

In addition to infusions of money into the tourism sector, there were initiatives to restructure small business (credit) debt. According to Mawdsley, Piza-Lopez, and Kaiser of the World Bank, “...Bank Indonesia published a decree in December 2002 asking banks to assist businesses in restructuring their credit. The Jakarta Initiative Task Force also held meetings and a conference in March 2003 with banks and businesses in Bali to promote debt restructuring between debtors and creditors.”\(^{85}\)

One such economic recovery program was directed at local small and middle-size businesses. Three Indonesian monetary institutions in Bali, Lembaga Perkreditan Desa (LDP),
Bank Rakyat Indonesia (BRI), and Bank Perkreditan Rakyat (BPR), issued lines of credit to small and middle-size business owners. However, the program suffered because of repayment problems many of those business owners subsequently experienced. Another Indonesian government backed program to aid in Bali’s recovery had, by 2004, either approved distribution of monies or had distributed monies to Balinese middle-size and small businesses by means of several government ministries that included Indonesia’s Department of Defense and Security. In the absence of clear program impact and outcome evaluations presented, it is not possible to evaluate the effectiveness of that program.

World Bank analysts suggested that broader structural problems such as the Asian economic crisis compounded economic hardships in East Java (and in Bali) to the point that the aforementioned Indonesian program might well have been imperiled from the start. For Mawdsley, Piza-Lopez, and Kaiser, “the effects of the Bali bombings are moreover overshadowed by a generally slow recovery of East Java in the wake of the Asian economic crisis after 1997-8.”

Hence, it seems likely that economic hardships, exacerbated by the Asian economic crisis and the SARS epidemic of 2002-2004, contributed to the growth of Islamic extremism for the reasons described above. In addition to this, it can be argued that economic hardship, in large part due to that economic crisis, impinged on the potential of some of these economic recovery programs’ capacities to work more effectively.

**Bali I – Lessons Learned**

There are several lessons that have been learned from the events of Bali I related to prevention; political/administrative, monetary, and legislative deficiencies; and preparedness and consequence management that will now be discussed.

**Prevention**

The political and economic effects of the Bali bombings compel us to think about prevention efforts taken by the Indonesian government and those not taken prior to the bombings. This chapter section distinguishes between political strategies that could have been taken prior to Bali I and some of the broader political and economic trends that worked to compound the economic effects of the Bali I bombings.

One set of opinions, as Balbi reports, expressed by Balinese after Bali I, was that Bali’s lack of economic diversity contributed to the problem. “One respondent,” as Balbi recalled, “spoke about how the bombings impacted thinking about the Bali economy, where it had jumped from an economy based on agriculture straight to a services economy, circumventing the industrialized economy, and how a reorientation was necessary to be better equipped for a disruption in the future.”

Clearly, that is a prescient argument — the introduction of flexibility into a local economy through diversification increases economic and societal resilience against external “shock effects” associated with terrorism or natural disasters. The multidimensional production conditions intrinsic to several product lines, even within firms, produces redundancy that allows worker transition in crisis situations into other economic sectors, if only on a temporary basis. The argument suggests the Indonesian national government should have worked to diversify Bali’s economy; a terrorist assault on the tourism industry without such strong reliance on the “services economy”, for example, would have caused much less economic devastation.

However, while the importance of economic diversification is an important lesson, such twenty-twenty hindsight does not take into account the broader political trends in Indonesia
that allowed Islamic extremism in Indonesia to grow in the first place. Major problems associated with political and economic reform prospects were apparent in, and intrinsic to, the Suharto era — characterized by political rigidity and overreliance on the military to cope with challenges to the regime. In authoritarian regimes, there is no “social compact” between the state and society to regulate ruling elite behaviors. Suharto’s manipulation of Islamic parties and movements for his own purposes prior to Bali I created conditions where Islamic extremism was able to take root and thrive.91

In his quest to find allies and political support, Suharto could not or would not recognize and distinguish adequately the number and depth of links between non-violent political parties and movements and more violence-prone Islamic extremist organizations. After Suharto’s resignation, there was continuous jockeying for political positions by Indonesian political parties and the military. The use of local Islamic militias (laskars) such as Laskar Jihad (LJ) by Indonesian officials to maintain law and order illuminated a dangerous situation. In the new, less authoritarian post-Suharto political landscape, heavy-handed actions to promote narrowly based interests continued to predominate as a style of rule. This precluded the prospect of more carefully reasoned approaches to address Indonesia’s collective political interests.92

**Political/Administrative, Monetary, and Legislative Deficiencies**

As previously mentioned, it seems likely that Indonesian government inaction against Islamic extremism was at least partially a result of the comparatively weak governments in place that followed Suharto, themselves characterized by reluctance to commit to post-9/11 US-led international and regional counterterrorism operations. The predominant reason why early post-Suharto governments were reluctant to cooperate more closely with the administration of President George W. Bush was because of the prevailing Indonesian public opinion that the US-led global war on terror was, in reality, a war against Islam.93

Ironically, the Bali I bombings produced an almost complete volte-face in Indonesian public opinion about the threat of Islamic extremism in Indonesia. After Bali I, it was possible for President Megawati Sukarnoputri to support the Global War on Terror more completely and, in the process, accept American and Australian assistance to augment Indonesian military and police anti-terrorism capabilities. From 2002 - 2008, the American money infusion amounted to $40 million, by contrast to $10 million provided by the Australian government.94 Those funds and other policing enhancement assistance made it possible for the Indonesian government to create the POLRI elite counterterrorism force Detachment 88 (Densus 88) that would, within the context of new legal powers, play a critical post Bali I role by arresting and killing JI leaders and activists.95

It is important to understand that Indonesian counterterrorism efforts included “soft-line” efforts at de-radicalization as well as “hardline” kinetic measures. Initially, international political leaders were concerned the Indonesian government would focus almost exclusively on broad, heavy-handed, “hardline” security responses, much in the style of a Suharto-like response. However, the emergent reality was the Indonesian government was also supportive of “soft-line” religious and cultural practices in Bali to promote community resilience, even though such religious and cultural practices were grassroots initiatives.96 As to why this happened, it is probably fair to say concerns over more democratic processes in the shadow of Suharto’s rule, in addition to the prospect of expected utility, at least in some de-radicalization cases, drove this softer policy approach.

A first mistake that contributed to Indonesian government inaction against Islamic extremism was its inability to fully appraise the profound problems that communal conflicts and separatism caused. Coupled with terrorism threats, these problems posed dangers to state security and integrity. Those twin threats dovetailed with the severe monetary constraints those conflict conditions imposed on successive Indonesian governments when it came to fight
homegrown Islamic extremism. For instance, it appeared that Indonesian officials like Vice President Hamzah Haz did not take the threat of Indonesian Islamic extremism seriously. In the case of Hamzah Haz, that was probably because of his own close ties to Islamic extremists.\(^7\)

This analysis highlights the confluence of interests and the political opportunities that galvanized after Suharto’s resignation to make it possible for Islamic extremists, and separatist group and ethnic group leaders, to coordinate their actions in pursuit of mutual gain. At a functional level, JI had embedded itself in Poso to provide protection to local Muslims afraid of Christian militias. In the contexts of nearly simultaneous conditions of communal conflict and separatism, where it was logical to assume leadership might share some interests, those connections became even more significant.

From the vantage of Indonesia’s government, the almost singular focus on those conflict conditions probably contributed to an outcome where the threat potential from those Islamic extremist group ties were downplayed.\(^8\) Indonesian officials somehow believed that if Bali had not been the target of attack within the context of those conflict conditions, then the likelihood of an attack remained very low. The logic of this argument was convoluted with the assumption that the drivers of both communal conflict terrorism were the same or very similar — as if a terrorist assault against the tourism epicenter that was Bali would result from the same set of communal conflict and separatism motivations.\(^9\) A role for “groupthink” and “perception and misperception” dynamics in upper-level Indonesian official circles with regards to these issues is a reasonable assumption — but remains speculative because of an absence of available data.

Those political and economic factors, as previously mentioned, aligned to produce a condition of stasis, where efforts to tackle Indonesian anti-American and anti-Western public opinion, characterized by acute anger at the US for its perceived war on Islam, were blocked outright. It should be noted that anger was most likely exacerbated by the confounding effects of economic hardship caused by the Asian economic crisis and the local economic backwater conditions left to fester by Presidents Sukarno and Suharto.

It is worth noting that the communal and separatist conflicts began to pass into eclipse from 2002 to 2005. This period leading up to Bali I was marked by anti-American sentiment, but even before Bali I, the Indonesian government had the opportunity to focus its attention on the threat posed by Indonesian Islamic extremists. Having said that, this era of communal conflict and separatism created profound national vulnerabilities for domestic Islamic extremists to exploit, amplified by the central government’s unwillingness to address the problem. That combination led to a policy where the Indonesian government used certain militias (lascar) to promote law and order. That policy also provided additional opportunities for Islamic extremists to establish networks, other connections, and to accrue resources.\(^10\)

Thus far, analysis points to incorrect or absent appraisals in the Suharto era about pernicious links between non-violent Islamist parties and movements and more extremist Islamic parties. The result was that extremist paramilitary elements in the guise of local militias were used to try to quell political instability, even in the post-Suharto era. The analysis points to fundamental misappraisals about the potential for militias that worked to defend Islamic communities in conflict with Christians, to establish relationships and networks with other more extremist Islamic militias.

The fact that Indonesian political parties and the Indonesian military made use of these Islamic militia and Islamic extremist groups to jockey for political position in the post-Suharto era reflects at best a makeshift and incomplete understanding of the deleterious political consequences of such behavior. This was most important for the Indonesian collective interest — development of civil society and of national institutions that were inclusive of, and responsive to, broad segments of Indonesian society.\(^11\)
The analysis points to a second set of post-Suharto regime problems that involve misappraisals and wishful thinking about the scope and degree of the specific nature of the Islamic threat in Indonesia from 1998 up through early 2002, prior to Bali I. This aspect of the Suharto-era style of government carried over into the early post-Suharto era and it was only a devastating terrorist attack at home that disturbed that indifference. There were other political and administrative "process" problems that stemmed from "nation-state" level factors that also contributed to the Bali I bombings. Those include institutional structural problems — an acute instability and organizational dysfunction linked to post-Suharto government fragilities and the anxieties of political leaders. For example, in reaction to the Suharto years, the visible presence of Indonesia’s military was curtailed by post-Suharto governments in efforts to put distance from the Suharto era with its heavy-handed use of military force. One manifestation of that was the 1998 split of Indonesia’s security forces into an army and a police wing, the TNI and POLRI. This contributed to dysfunction — "turf war" competition between the Indonesian National Police (POLRI) and the Indonesian National Army (TNI), as opinions between the military and national police differed about each organization’s overall capabilities, effectiveness, and scope of responsibilities. That instability, coupled with the overall weakness of those post-Suharto governments with its leadership insecurities, contributed to decisions that led to extremely poor security preparations in Bali. One result of this new organizational security approach was that in Bali, community-based paramilitary organizations known as pecalang that were poorly trained and organized, oftentimes stepped into the security vacuum to perform law-and-order functions. The pecalang were local militia with a reputation for discrimination against Balinese street merchants, vendors, and other non-Balinese. The vulnerabilities that derived from the flawed appraisals of the terrorism threat at the top echelon of the state by early post-Suharto national governments, bound up with the drastic reduction in visible military presence throughout Indonesia — clearly a political move as a result of the "reformation" — most likely created counterterrorism infrastructure and response vulnerabilities. The lack of effective security infrastructure prior to Bali I was paralleled by the lack of effective legal instruments at that time necessary to prosecute terrorists. Both reflected the lack of counterterrorism focus that was the hallmark of post-Suharto governments prior to 9/11. The Indonesian judicial landscape prior to Bali I was marked by makeshift and incomplete legal instruments. These are perhaps best reflected by the emergent reality that the United Nations Security Council (UNSC) passed a binding resolution that declared JI a terrorist group in 1996, and the Indonesian government did not follow suit until April 2008, with a magistrate’s ruling in District Court in South Jakarta. Thus, it was only after Bali I that the counterterrorism legislative void was filled. After Bali I, President Megawati Sukarnoputri’s emergency measures were codified into law by the Indonesian parliament in counterterrorism legislation passed in March 2003. For Johnson, those watershed legal events reinforced the primacy of the police approach and apparatus over the military, an approach that also made use of “soft-line” counterterrorist measures. Those legal instruments included provisions where government capacities to collect inculpative evidence were expanded, and where in the process, terrorist suspects could be imprisoned for a maximum of six months.

Preparedness and Consequence Management

In this section, the discussion about how to protect commercial interests is largely speculative — it revolves around the notion of what initiatives might have been taken by various stakeholders prior to Bali I to improve their economic standing in the aftermath of the Bali I bombings. As indicated before, lack of a visible military presence was both a cause and an effect of new political conditions and a source of the political uncertainties associated with
Suharto’s resignation. This section explores what indirect economic benefit could have accrued with a more visible military presence in Bali and associated consequences.

Asongu and Nwachukwu’s work suggests emphasis on the visible presence of Indonesian “armed service personnel” rather than more reliance on law enforcement in Bali might have increased tourist arrivals there after the Bali I and Bali II bombings because of the perception among tourists that with the military present, they could feel more secure. Asongu and Nwachukwu’s results run counter to sentiments of the early post-Suharto governments to reduce military presence to distance themselves from Suharto and suggest that from a purely economic security standpoint — and most likely from a traditional security standpoint — the reduction in visible military presence policy might have been a mistake.

In contrast, Ghaderi, Saboori, and Khoshkam’s findings have particular relevance for post-Bali I and post-Bali II conditions. Ghaderi et al.’s findings illustrate an inverse relationship between a unit change in “aggregate security” and tourist arrivals in developing countries. In other words, a one unit increase in “aggregate security” leads to a decrease in tourist arrivals in developing states of about four percent. Ghaderi et al.’s work suggests that while security focus is critical to ensure tourist flows, “….other factors such as travel cost, visa facilitation, emerging exotic and attractive destinations have been influential.”

Thus for Bali to achieve greater economic security, the security required is two-dimensional. First, this can be with direct inputs to economic security where POLRI or TNI (or both) assume control over many traditional security functions rather than having the pecalang or an organization like it handle functions. Second, is that indirect inputs such as low travel and hotel accommodation costs, favorable exchange rates, and easy-to-obtain visas remain instruments available to maintain higher levels of tourist arrivals. In other words, traditional security is a necessary but insufficient condition for economic sustainability and robust resilience against terrorist attacks. The challenge here is those types of initiatives require significant public-private partnership frameworks. That, in turn, requires a developed private sector whose leaders are willing and are able to engage in efforts that amount to corporate social responsibility (CSR). That has proven difficult even in some developed countries such as the US.

For businesses, anticipatory, government-sponsored insurance programs in Indonesia orchestrated with the assistance of government and non-state actors might be fruitful. Anti-terrorism insurance policies have the potential to offset the extensive damage to the tourism industry and related commercial interests. An Indonesian insurance program akin to the American Terrorism Risk Insurance Act (TRIA) might have established a set of insurance baselines to stipulate levels of premiums to be paid by private sector companies before government subsidies to provide monies for rebuilding would kick in to make compensation to economically victimized business owners viable. One additional part of such a program might also include insurance provisions in anticipation of foreign tourist kidnappings.

However, the problem here revolves around the comparatively weak tax systems in many developing countries such as Indonesia to fund such programs. This is because, as in the case of a program like TRIA, the overall cost of an insurance program to combat the effects of “spectacular” terrorist assaults is ultimately passed along to policyholders (i.e., the consumer) with premium increases, and, ultimately, to the population at large with moderate increases in taxes to fund such programs. As some 16 percent of Indonesians lived in poverty, this policy option alternative is problematic without taking into account outside donor support. Perhaps one option would be to involve multinational corporations (MNCs) more heavily in the counterterrorism security policy process to develop bulwarks of economic protection where both MNCs and state/societal interests are met.

In essence, what that condition suggests is the establishment of a worldwide counterterrorism insurance program funded by several donors: ASEAN, the World Bank, the International Monetary Fund (IMF), the Islamic Development Bank, and the Asian...
Infrastructure Investment Bank (AIIB) for instance. Such an insurance program would service commercial sector victims of terrorist assaults in countries that do not have sufficient economic strength to undertake such programs on their own. Heiduk provides a roadmap of sorts—in his description of more indirect EU influence on security relations with the Association of Southeast Asian Nations (ASEAN)—outlining five collaborative areas: “judicial cooperation,” “migration and border management,” “intelligence cooperation,” “combating terrorist financing,” and “law enforcement.”

That approach is consistent with the clarion call by scholars for additional multilateral efforts to confront “twenty-first century problems,” as Kaplan puts it, such as terrorism, drug trafficking, illegal arms trafficking, human trafficking, and climate change that cross over national borders. Those initiatives should be taken in conjunction with continued national efforts, supported by outside donors to strengthen Indonesian civil society and, in the process, spur on continued development of more effective national institutions. In specific terms, what that means is that professional and social institutions such as lawyer guilds, women’s rights and children’s rights organizations, and institutions to assist the poor, for example, must be encouraged to thrive unfettered from government interference.

Another lesson related to business preparedness and consequence management already briefly touched on above, draws from Gurtner’s work on corporate social responsibility (CSR) measures that could be taken by large-scale business organizations operating in and with Bali. Gurtner suggests that CSR programs in the pre-Bali I bombing context might have contributed to consequence management by making educational opportunities and vocational retraining programs available to Balinese workers, thereby working to increase economic redundancy and societal (and governmental) resilience. Gurtner suggested programs might be funded by the Indonesian national government, perhaps in conjunction with the IMF or the World Bank or with regional intergovernmental organizations (IGOs) or a combination thereof to generate revenue.

To be sure, many of the problems that ultimately led to a failure to prepare adequately for an event like the Bali I bombings involved policy decisions (or the absence thereof) on the part of the national government that focused its attention at the time on heavy-handed measures to quell threats to national security stemming from communal conflicts and separatism. One lesson to learn is that “hardline” counterterrorism must be augmented with “soft-line” counterterrorism with a focus on political/administrative, judicial, economic, and legislative responses working in coordinated fashion and, if needed, with “hardline” efforts when those “hardline” efforts are really required.

The tragedy is that the separatist calls for self-determination in Aceh and the fundamentally different separatism in East Timor calling for freedom from Indonesian military occupation. East Timor was originally not a part of Indonesia. The call for protection of natural resources in the case of West Papua, and the communal conflict in places such as Ambon, Poso, and Maluku, came on the heels of structural political change in Jakarta, Indonesia’s political epicenter. Had the roots of the fledgling Indonesian democracy run deeper, those events might have been able to be met with negotiation processes in the case of the former and peacekeeping operations rather than suppression strategies in the case of the latter.

The Bali II Bombings (2005)

The Bali II bombings occurred on 1 October 2005, in south Bali, at two family-run eateries in Jimbaran Beach and at a restaurant in the central square of Kuta. Those bombings were carried out by an allied splinter group of Jama’ah Islamiya (JI) known as al-Qaeda in the Malay Archipelago (Tanzim Qaedaat al-Jihad), and led by Malaysian JI leader Noordin Mohammad Top. Top was a former JI commander who had been a principal in the Bali I bombings. The Bali II bombings caused much less carnage than the Bali I bombings — twenty people died,
while over one hundred others were wounded (in the first Bali bombings, 202 people were killed and another 200 wounded).\textsuperscript{117}

What is significant here is the Bali II bombings occurred within the context of substantial change in the structural shape of JI, and of a much-strengthened Indonesian state that by then had the overwhelming support of its citizens following the public’s reaction to the Bali I bombings. Even prior to the Bali I bombings, cleavages existed in JI between leaders with fundamental differences in opinion regarding their strategic approach and the overall pace of action. Prior to Bali I, such cleavages existed between leaders of “Mantiqi I,” JI’s organizational division for Singapore, Southern Thailand, and Malaysia, who advocated for an immediate campaign of violence, and leaders from Indonesia’s Sumatra and Java regions in “Mantiqi II,” who advocated for incremental political change, at least for the immediate future.\textsuperscript{118}

Those JI cleavages became more pronounced in 2002 — some “non-structuralist” JI leaders such as Noordin Top wanted to pursue a global agenda of offensive action to be taken immediately, akin to the al-Qaeda model of confronting the “far-enemy.” In contrast, “structuralist” JI leaders, as Gordon and Lindo put it, believed the best course of action after Bali I was, at least temporarily, to pursue incremental change politically, with more local focus on Indonesia and Southeast Asia. At the same time, those JI activists did not renounce violence formally, but postponed the use of violent attacks until a more propitious time.\textsuperscript{119}

Still, as Gordon and Lindo have pointed out, this was a separation characterized more by subtleties and nuance, rather than by a strict separation tantamount to a complete divorce, a notion popularized and embraced by some Indonesian political leaders, as well as the Indonesian public. “In fact,” as the authors found, “Non-Structuralist JI members were products of JI-linked schools, consumers of JI publications, and frequently drew on their relationships with other JI members.”\textsuperscript{120}

Plainly, printing JI documents, running schools, and maintain membership networks required money. In time, JI monetary problems became so dire that public donations, rather than reliance on large sums of money from selective donors, many of whom were now incarcerated, were used to help maintain JI coffers. With the arrest of JI leader Zulkarnaen in December 2020, a network of 20,000 charity boxes in Indonesia, tied to a JI shell organization called “Abdurrachman bin auf” for anonymity purposes, was exposed. Those donations, along with the profits made by JI front businesses selling consumer goods such as palm oil, had become a primary source of JI funding. In addition to the provision of military training and weapons procurement, some authorities believe those monies were held in reserve by JI “structuralist” leaders for a new JI foray into Indonesia’s political system in the not-so-distant future.\textsuperscript{121}

JI leaders from the “JI Structuralist” branch included Abu Bakr Ba’asyir, who in 2008 had established what was an ostensibly non-violent JI splinter group called “Partisans of Oneness of God” (Jemaah Ansharud Tauhid — JAT).\textsuperscript{122} Nugroho described JAT as essentially “Janus-faced” with respect to its position on the use of violence. Because, while JAT’s upper-echelon leadership ostensibly placed emphasis on non-violent activities holding theoretical discussions about the role of Sharia law for Indonesia and in broader Southeast Asia in publications, conferences, and promotion of religious schools, that leadership still had connections to Islamic extremist organizations and supported those groups.\textsuperscript{123}

In fact, Gunaratna and Petho-Kiss report that from 2018-2020, Jemmah Ansharud Tauhid (JAT) linked terrorist assaults in Indonesia declined, perhaps partially due to the Coronavirus pandemic, a finding the authors note is consistent with declining terrorist assault rates for many other terrorist organizations in that period. Gunaratna and Petho-Kiss also point to pandemic-related divisions over policy direction within JAT and the arrest of 57-suspected JAT activists as other factors that might have contributed to decline in JAT’s terrorist attack frequency rate.\textsuperscript{124}
The establishment of JAT, and with it the notion of what Lasswell might call a JI "maturity cycle" evolution, is particularly notable because the process whereby a non-violent splinter group emerges from a terrorist parent group reflects the importance of “contextual factors” at work. In this case, this was a newly strengthened and rejuvenated Indonesian national government backed by popular support, with a sharp focus on efforts to tackle domestic Islamic extremism. In addition, those efforts were buttressed by American political, military, and economic assistance, and Australian political, economic, and police assistance from the Australian Federal Police.

The Bali II Operation and Economic Effects

It was during the time of President Susilo Bambang Yudhoyono’s government that the Bali II operation was orchestrated by Noordin Mohammad Top. Noordin Top was assisted by his second-in-command leader known as Ubeid, and with the help of Dalmutin, a close Islamic extremist confederate. Top was also assisted by Dr. Azhari bin Husin (aka Azhari), a high-level participant in the Bali I bombings, who was the chief bomb maker for JI. According to Nugroho, who cites Klaimanee and Nogaj, Top’s JI splinter group was small, comprised of only 79 activists.

As Gordon and Lindo, and the International Crisis Group report, both Azhari and Top hid in various parts of West Java, continuously on the run from Indonesian security authorities for three years since the Bali I attack. There were several crucial members of this team that included Noordin Top, Ubeid, Dr. Azhari, Jabir, Cholily, Agus Pururyanto (aka Arman), and the suicide bombers Aip Hidayat, Misro, and Salik Firdaus. As previously mentioned, Al-Qaeda in the Malay Archipelago was one of several “non-structuralist” JI splinter groups that emerged after 2002, led by former JI chieftains such as Noordin Top and Umar Patek.

According to Johnson, Top had strong administrative skills; he was able to work with a range of Islamic extremists from different organizations under the banner of Al-Qaeda in the Malay Archipelago. It was probably Top and Azhari, perhaps through Jabir, who brought Cholily, a university-age student, into the orbit of Al-Qaeda in the Malay Archipelago (Tanzim Qaedat al Jihad), even though one news account reports that Ahmad Basyir, a member of KOMPAK, itself a DDII “Islamic relief agency,” was responsible for Cholily’s entry into the Top-Azhari fold.

Cholily served as Azhari’s protégé, helping to construct the backpack bombs that would be used, filled with shrapnel, including ball bearings. There were also several other unexploded devices found by police after the 2005 attacks. If that account about Cholily’s enlistment into the al-Qaeda in the Malay Archipelago is accurate, that KOMPAK connection, in addition to the enlistment of Agus Pururyanto, who had prior DDII experience, resonates with the permeability dynamics between non-violent and violent extremist groups previously mentioned.

It was Agus Pururyanto (aka Arman) who helped Top and Azhari with the necessary logistics for the implementation of the terrorist plot, such as finding lodgings for Azhari in Solo, where he lived up to a few months before the Bali II bombings. Azhari also hired Jabir, another logistics specialist, who in turn enlisted the three suicide bombers: Aip Hidayat, Misro, and Salik Firdaus, the latter being one of Jabir’s students from the Darusyahada pesantran (religious school), near Solo.

What is significant here is the reaction to the Bali II terrorist assaults picked up where the Bali I bombings left off; it served to increase the intensity of the Indonesian public’s rejection of Islamic extremism even further. Consequently, Indonesia’s national police (POLRI) was given more operational “political space” provided by new counterterrorism legislation. Its new operational Detachment 88 became the lead agency in countering terrorism in Indonesia. As a
result, POLRI worked much more smoothly with the military and managed to eliminate JI as a significant threat to Indonesian security in the aftermath of the second Bali bombings.

One measure of how conditions had changed profoundly since the pre-Bali I era was the capacity of Bali’s local police to participate in national efforts to investigate Bali II and continue with its own efforts, with advice and consent from Indonesian national security forces. Balbi reports there was a new security consciousness in Bali after the Bali I bombings. It made Balinese people more sensitive to terrorism’s threat potential, no doubt spurred on by a profound and lasting guilt that many Balinese experienced. Having said that, both Nugroho and Chalk and Ungerer suggest that the formidable and largely successful police and military operations against JI in the post-Bali I and Bali II eras, do not take away the risk that lone operative terrorists will continue the struggle on their own, motivated by JI’s jihadist message.

The international economic effects of Bali I in terms of tourist arrival rates were somewhat larger than the effects Bali II had on that rate, with a 20 percent decline as compared to the 25 percent drop in the case of Bali I bombings. Still, the generally recognizable effect of the Bali II bombings was to compound the local economic effects of the Bali I bombings for the hotel management sector, the airline sector (to Bali), and small shops and services related to those sectors that catered to tourists.

Many hotel and bar operations, significantly impacted after Bali I, were forced to close or significantly curtail operations with the end result that many local families were affected even more profoundly than before. For example, some informal industries such as the Bali “beach cowboys,” where young men who worked to make amorous connections primarily with wealthy Western women, essentially disappeared. Bali as a tourist venue has never fully recovered economically from the bombings, with Australian and American tourists encumbered by continual security concerns and, as Balbi reports, fundamental differences of opinion about how to memorialize the victims of the bombings.

In terms of lessons learned, one set of lessons intrinsic to the comparatively low levels of economic damage caused by the Bali II bombings derives from the importance of structural political factors at the national level that changed significantly after the Bali I bombings. The effects of the structural transition from Suharto’s authoritarian regime to the post-Suharto governments that created problems with identification of domestic terrorism had faded along with concerns about intensive communal conflict and separatism. As those worries passed into eclipse and especially after the Bali I bombings, a change of groundswell public opinion made it possible for Megawati to support fully American-led efforts to respond to global terrorism.

Equally important, the opportunity that this shift in public opinion made for Megawati was to accept and make use of the counterterrorism assistance provided primarily by the US and Australia. By the time that Bali II happened, a new security apparatus was operational, already working successfully to destroy JI and tackle the challenges associated with violent “non-structuralist” JI splinter groups such as al-Qaeda in the Malay Archipelago. In addition, the significant macro-economic effects of the Asian economic crisis (1997-98) had begun to pass into eclipse by 2005. Analysts reported continued confidence about the global economy; moreover, the Jakarta stock market index increased 0.38 percent some two days after the Bali II bombings.

Still, the economic malaise in Indonesia continued with enormous distance between the “haves” and the “have nots” exposed starkly by globalization processes, with effects that probably continued to amplify the disaffection of many urban dwellers about particular economic predicaments such as housing. However, government efforts to uproot JI after the Bali I bombings dovetailed with the abatement of Asian economic crisis effects to probably make living conditions in Indonesian cities at least a little more tolerable or financially stable for many.
It appears that state level factors that aligned to allow for the growth of the threat of domestic Islamic extremists — which had culminated in the Bali I and II bombings — had now fallen out of alignment and that some international level macro-economic factor effects that coincided with those problems did the same. For example, the acute nature of the Asian economic crisis and the SARS crisis had dissipated even though the GWOT continued. While some of the decisions made, especially during the Suharto era and by early post-Suharto governments about political power acquisition, were disturbing and clearly detrimental to the long-haul stability of Indonesia, some comfort can be taken. The reason why is because if those lessons are taken to heart, the end result is an increased understanding about the importance of civil society and democratization to political stability, both nested in more effective Indonesian national and local institutions. The rationale behind this is that to ease domestic pressures, increased availability of political and economic “opportunity structures” can help to reduce pressures that for some contribute to processes whereby people enter into the orbit of terrorism.

Final Reflections

An appraisal of the Bali I bombings and the Bali II bombings appears to illustrate that several Indonesian national political factors had effects that converged to pave the way for Islamic Jihadism in general and Jama’ah Islamiya in particular to grow. Moreover, effects of those explanatory factors were amplified by a confluence of international level system factors to multiply political grievances and to exacerbate economic hardships. Nugroho, who draws on work by both Pape and Stern, suggests that the 2003 Iraq invasion accelerated JI recruitment because the GWOT, with what Hudson calls its emphasis on “regime change” and its “military style” approach, proved to be less effective in many instances than counterterrorism programs with the police rather than the military in the lead.

Those macro-political factors and effects, both at the state and international level, are multifaceted and interconnected in complex ways. First, Suharto’s resignation (1998) created a structural shift in Indonesian politics that opened up several opportunities for malignant Islamic extremist organizations to grow unfettered. Competing interests between political parties, government-sanctioned Islamic organizations such as Nahdlatul Ulama and Muhammadiya, and the Indonesian military in the immediate post-Suharto era not only allowed domestic Islamic extremism to grow — it also obfuscated existing problems both within a dysfunctional political system and across the political landscape.

Not only was the fierce competition between political parties and the military a problem, but the process at the heart of that competition reflective of Indonesia’s pronounced problem with corruption compounded the problem even more. It is worth nothing that the willingness of those parties to exploit a condition characterized by non-violent and violent Islamic parties and movements was tied with the aim to gain political support and advantage. Plainly, the inability or unwillingness of government actors to acknowledge those connections created a condition where Islamic extremists could continue to grow apace. This problem was compounded by the inability of those weak early post-Suharto national governments in Jakarta to exert full political control in many areas far from Jakarta.

In terms of economic impact, the Bali I bombing demonstrates the economic ripple effects that even a single terrorist event can have on entire regions. In this case, local tourism in Bali was affected most profoundly, but the hotel and airline industries in the region also suffered as tourism declined significantly for up to two years after the bombings. While regional tourism from Japanese and Singaporean tourists, for example, helped to compensate to some degree, it did not offset those losses.

The losses incurred in Bali I were compounded by the Bali II bombings in both economic and psychological domains, even though the economic destruction and disruption caused by
Bali II was not nearly as large. A direct consequence of the Bali II bombings was a continued loss of consumer confidence in travel to Bali, with consumers looking for “second best alternatives” to reclaim the glamor, romance, and similar sentiments associated with Bali. As Schmid points out, “customers of tourist products are flexible while tourist destinations — except for cruise ships — cannot move.” It appears the prevailing result of the Bali II bombings was psychological, compounding the economic problems in Bali already in place, because what were initially more optimistic appraisals made about Bali’s future after the Bali I bombings were completely shattered.

What the foregoing suggests policy-wise in efforts to confront terrorism is that Indonesian leaders must work to ensure that the rudiments of civil society, which began to take hold after the overthrow of Suharto, continue to grow more deeply into the Indonesian political landscape. What that means is a condition where there is a high degree of tolerance for political and social institutions that represent women’s and children’s rights and the poor, for example, to operate unfettered by government interference. Political and economic “opportunity structures” must be available to channel, at least for some, what Dollard et al. would call the “frustration and aggression” associated with willingness to enter into the orbit of terrorism.

This becomes even more important within the context of successful police, military, and judicial prosecution against JI in the post-Bali I and Bali II periods.

In fact, Nugroho, Chalk, and Ungerer argue plausibly that lone operatives or small groups could continue the struggle. That problem is compounded even more because of long-standing JI interest in biological and chemical weapons development. Gunaratna and Petho-Kiss report that following 9/11, a JI handbook about biological and chemical pathogens (written by authors such as JI biologist Mustaqum) was discovered in Mindanao, Philippines. Moreover, in August 2004, Mohamad Fadzullah Abdul Razak, a Malaysian engineer inspired by JI, tried to cultivate Botulinum; he then sent his garden variety Botulinum spores in laced envelopes to several diplomatic legations, including the US embassy in Kuala Lumpur.

Overlaid against the basic weakness of effective political institutionalization where political parties and bureaucracies are representative of different segments of society and respond to political demands and aspirations, the unresolved political role of the military and other macro-political factors in the Indonesian national context make control over these conditions even more difficult. The growth and outbreak of communal conflict and sub-national separatism severely constrained finite military and political resources, making it more difficult to combat Islamic extremism, even if it had been acknowledged as a problem in the early post-Suharto years — which it was not.

All of the foregoing played out against the backdrop of broader international political system factor effects. The Global War on Terrorism (GWOT) created an anti-American political environment for most Indonesians. This, in turn, inhibited Indonesian leaders from meaningful participation against Islamic militancy; that prevailing sentiment would not change until after the Bali I bombings (2002). In the case of Indonesia, the standard neo-realist “three level analysis” of conflict, with “international” (Waltz’s “third image”), “nation-state” (Waltz’s “second image”), and “individual level” (Waltz’s “first image”) factors, has served as the basis of this analysis to illustrate factors and their effects that interact within and across levels, working to explain sources of conflict.

To explain events in Indonesia leading up to the emergence of JI and the Bali bombings, primary emphasis is placed on “international political system” and “nation-state” level factors. There was a reinforcing effect between the explanatory variables found at the “international political system” level (such as the Global War on Terrorism, the Asian economic crisis, and even the SARS virus) coupled with political and economic conditions at the “nation-state” level of analysis - which all worked to make the threat of JI so virulent.

Notwithstanding that, focus on the “individual level” of analysis (Waltz’s “first image”) is also crucial as efforts by the Indonesian political and military leadership to downplay dangers
associated with the rise of Islamic extremism appear to have been driven by individual and small, upper-crust decision-making processes. Decision or indecision about the threat of Islamic extremism might have gained traction through conformity in thinking pressures and processes captured in Irving Janis’s notion of “groupthink,” stimulated by the seemingly more urgent need to focus on separatism and communal conflict.145 Moreover, the outright denial by some political figures (such as President Megawati’s sister) about the threat posed by domestic Islamic extremism and reliance on conspiracy theories about a US war on Islam, that was commonplace to note, fits well with Robert Jervis’s notion of “perception and misperception.” This notion addresses incoming flows of information at odds with preexisting beliefs and norms that cause a condition of “cognitive dissonance,” where psychological processes to make unpleasant information flows manageable and tolerable are triggered.146

If the Global War on Terror heightened political grievances and subsequent political demands and aspirations due to the mistaken belief, that it was a war against Islam. Subsequently, the Asian economic crisis and to a much lesser degree the SARS virus outbreak exacerbated local economic conditions to create economic hardships that made Islamic extremism more seductive as an answer to political problems. For some, Islamic extremism worked to provide identity and political/social place in the Indonesian polity whose norms and values, and political processes, were evolving after Suharto’s fall.

Indonesian government and society experienced this shift in political norms, process, and function in ways that resonate with Durkheim’s notion of “anomie.”147 In post-Suharto Indonesia, there was an unfortunate alignment of “international political system” factors and “nation-state” level factors that resulted in a very narrow range of effective policy options that could be implemented by early post-Suharto governments to attenuate the growth of Islamic extremists. The economic effects of Bali I were enormous, and while certain economic programs in response to Bali I had the potential to work more effectively, pre-existing economic conditions, coupled with weak national government agencies, made the likelihood of new post-Suharto economic recovery program success, even with substantial international assistance infused into the system, tenuous at best.

The lessons learned are that first, the alignment of “nation-state” and “international political system” factors can indeed happen with the result of ineffective national security and counterterrorism conditions. Those fragile institutions and processes can pave the way for calamitous domestic developments that fill vacuums created by structural political change. What that requires is anticipatory governance with an emphasis on contingency planning to anticipate different alignment conditions with carefully reasoned consideration of alternate scenarios. At the heart of those scenarios are efforts to harden core economic interests and networks of interconnections to service sectors places like Bali.

One way of thinking about the problem involves “smart city” development and applications tailor-made to local conditions. The term suggests a framework of interactive institutions within the boundaries of a city or cluster of cities readily accessible to respond “in real time” to citizen inputs, through kiosks for example, with security alert functions and capacities to process administrative proposals made by ordinary citizens about how to improve municipal effectiveness and efficiency. The goal is a stakeholder pool that is broad and deep — with professional policymakers and ordinary citizens making contributions about security as it pertains to the mixture of residential and commercial infrastructure, available “urban space,” and the security vulnerabilities created. These standpoints as well as tactical instruments of protection such as sensors, biometrics, and CCTV networks, could be used to protect against the economic consequences of terrorist assaults.148

While the argument can be made Bali II was a second chapter or continuation of the Bali I experience, it is not an especially useful statement to make because Bali II happened against the backdrop of the split between “Structuralist JI” chieftains who decided to suspend the armed struggle against the West and Southeast Asian governments for the time being, and
“non-structuralist JI” leaders who opted to continue the armed struggle along the lines of the Al-Qaeda model. Bali I made it possible for President Megawati to retool her security apparatus primarily with American and Australian help. In turn, those windows of opportunity emerged because of changes in international factor effects — Bali I, the emergent reality that communal conflict and national separatism was beginning to pass into eclipse, and the reduction of at least some of the negative macroeconomic effects that stemmed primarily from the Asian economic crisis.

It follows the final lesson learned from the Bali bombings is the importance of foresight — formulation and implementation of national and multilateral efforts to prepare for “spectacular” terrorist assaults ahead of time, to confront the economic ripple effects of terrorism, which are especially pronounced in a world of intensive globalization. Economic diversification efforts, especially crucial to small area economies dominated by one industry, is critical. As previously mentioned, anticipatory governance processes in place might have detected the lack of economic diversity and depth in Bali during the pre-Bali bombing eras with recommendations to diversify and create redundancy in the system, and in the process increase government and societal resilience.

In addition, another anticipatory foresight program recommended revolves around the creation of an internationally based insurance program with international resources to be donated by countries, MNCs, and IGOs — the EU, ASEAN, the World Bank, the UN, or the G-20, for example, to provide more effective coverage for small and medium-size businesses to cope with economic losses incurred. Foresight as an intrinsic component of public policy formulation and implementation would work to save untold sums lost to “spectacular” terrorist assaults and sustained terrorism campaigns. This component of a new “multilateralism” in the twenty-first century contemporary world is desperately needed, but has become increasingly elusive since the outbreak of the Coronavirus pandemic.

Richard J. Chasdi is a Professorial Lecturer, Department of Political Science, George Washington University. He is also an Adjunct Senior Fellow, International Center for Political Violence and Terrorism Research (ICPVTR) at the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, Singapore. Prior to that, Dr. Chasdi was a Professor of Management at Walsh College, Troy, Michigan. He received his B.A. in politics from Brandeis University in 1981, his M.A. in Political Science from Boston College in 1985, and his Ph.D. in Political Science from Purdue University in 1995. He has published four books on terrorism and counterterrorism, and several book chapters and refereed academic articles. Chasdi’s first book, “Serenade of Suffering: A Portrait of Middle East Terrorism, 1968-1993” (Lexington Books, 1999) received Choice magazine’s “Outstanding Academic Title” in the field of International Relations in 2000. Dr. Chasdi serves on the editorial boards of “Perspectives on Terrorism and Armed Forces & Society”. In 2017, Chasdi was a Fulbright Specialist at RSIS at Nanyang Technological University, working as a Visiting Fellow at the International Centre for Political Violence and Terrorism Research (ICPVTR). He has served as a news consultant for various radio and TV stations in the United States and abroad.
Appendix I — A Typology of Terrorism’s Economic Disruptions

Work to conceptualize and categorize specific types of economic disruption caused by terrorism is enhanced by a three-dimensional typology, “A Typology of Terrorism’s Economic Disruptions.” This typology has three distinguishing characteristics: A. “Target Industry”; B. “Scope”; and C. “Time Interval.” The first distinguishing characteristic, “Target Industry,” is broken down into six industries: tourism; transportation; food/water production and distribution; banking/finance; medical facilities; and private housing and commercial stock. The first of these designations — “Tourism” — is inclusive of hotel management and allied sub-industries such as amusement parks, nature reserves, and other sightseeing locales and operations.

The second industry category is “Transportation” — with focus on the economic repercussions of terrorism against airliners, airports, buses, cruise ships, trains, and related infrastructure such as airports, train stations, bus terminals, and harbors. In addition, taxis, Ubers, and the revenue shares of taxi and Uber-related travel en route to airports or helicopter pads are included. The third industry is “Food/water production and distribution.” This industry category takes into account production, distribution, maintenance of food and water supplies, as well as water purification.

In turn, “Banking and/or finance” is the fourth industry category, inclusive of a range of financial institutions, including stock and bond markets susceptible to economic disruptions from terrorist assaults. The fifth industry category is “Medical facilities”, inclusive of economic repercussions from terrorism on hospitals budgets, first-responder budgets, and related infrastructure such as the capacity to procure sufficient respirators or personal protection equipment (PPE), dramatically underscored by the recent Coronavirus pandemic. Finally, the sixth articulated industry category is “Commercial and/or private housing stock” where economic disruptions caused by terrorism translate into rent changes and stock availability, primarily as a function of diminished supply.\(^\text{151}\)

The second distinguishing characteristic is the “Scope” of economic effects caused by terrorism. This distinguishing characteristic of “scope” is broken down into six sub-categories that articulate ranges of scope relative to nation-states. The first of those is “national economic effects,” that are inclusive of aggregate effects to specific states, provinces, or departments. The second sub-category, “regional effects,” captures economic effects that span regions, namely across national economies in generally recognizable geographical areas.\(^\text{152}\)

The third sub-category is “International economic effects,” that captures disruptions in volume of trade and world economy size and growth. For example, “spectacular” terrorist events such as 9/11, the 2002 Bali bombings, the 2004 Madrid bombings, the 2005 London “7/7” bombings, and the 2008 Mumbai attacks have international economic repercussions on one or more of the target industries listed above - such as “tourism” or “transportation.” In turn, the fourth, fifth, and sixth categories respectively are “international effects and regional effects,” “international effects, but with no regional effects,” and “no international effects” but with regional effects.

The third distinguishing characteristic in this typology is “time interval.” Time interval is broken down into “short-run”, “middle-run”, and “long-haul” periods even though many scholars debate whether or not terrorist events, over and beyond “ultra-spectacular” events such as 9/11, have long-haul economic or political implications or both. Hence, this “Typology of Terrorism’s Economic Disruptions,” is a three-dimensional 6x6x3 cube-like structure with 108 possible iterations, many of them found in the larger world of action. It should be noted that while the typology can be modified to take into account multiple terrorist target assaults in future work, the typology in its present form can only take into account single-target-type attacks. From those 108 iterations, the ones that can be found in the larger world of action can
serve as the basis of hypothesis formation (theoretical propositions) in future work that can be crafted and tested empirically.¹⁵³

Typology of Terrorism’s Economic Disruptions (sample of 108 iterations):

1. A1 B1 C1 – 1, 1, 1 — economic disruption effects of a terrorist assault against a tourist target with national effects in a short-run time interval.
2. A1 B1 C2 – 1, 1, 2 — economic disruption effects of a terrorist assault against a tourist target with national effects in a middle-run time interval.
3. A1 B1 C3 – 1, 1, 3 — economic disruption effects of a terrorist assault against a tourist target with national effects in a long-haul time interval.
4. A1 B2 C1 – 1, 2, 1 — economic disruption effects of a terrorist assault against a tourist target with regional effects in a short-run time interval.
5. A1 B2 C2 – 1, 2, 2 — economic disruption effects of a terrorist assault against a tourist target with regional effects in a middle-run time interval.
6. A1 B2 C3 – 1, 2, 3 — economic disruption effects of a terrorist assault against a tourist target with regional effects in a long-haul time interval.
7. A1 B3 C1 – 1, 3, 1 — economic disruption effects of a terrorist assault against a tourist target with international economic effects in a short-run interval.
8. A1 B3 C2 – 1, 3, 2 — economic disruption effects of a terrorist assault against a tourist target with international economic effects in a middle-run time interval.
9. A1 B3 C3 – 1, 3, 3 — economic disruption effects of a terrorist assault against a tourist target with international economic effects over a long-haul time interval.
10. A1 B4 C1 – 1, 4, 1 — economic disruption effects of a terrorist assault against a tourist target with international effects and/or regional effects in a short-run time interval.
11. A1 B4 C2 – 1, 4, 2 — economic disruption effects of a terrorist assault against a tourist target with international and national effect and/or regional effects in a middle-run time interval.
12. A1 B4 C3 – 1, 4, 3 — economic disruption effects of a terrorist assault against a tourist target with international and national effect and/or regional effects in a long-haul interval.
Endnotes


6 Ibid.

7 Schmid, 2013, p. 212.


10 Ibid., p. 25, pp. 48-50. A one standard deviation increase in domestic terrorism (per 100 people) affects FDI/GDP more than a one standard deviation increase of transnational terrorism (per 100,000 people).

11 Ibid.


13 Ibid.

14 Lakdawalla and Zanjani, 2002, p. 4. The authors find government insurance subsidy strategies dovetail well with “public law enforcement strategies.”

15 Ibid.


17 Ibid., p. 6.


---


25 Nahdlatul Ulama and Muhammadiya are non-violent government-sanctioned Islamic bodies that practice “moderate” Islam, but Nahdlatul Ulama is oriented towards rural Indonesians with its “traditionalist” standpoint. This in contrast to Muhammadiya, that is urban oriented and, hence, “modernist.”


36 Ibid., p. 186 n.725, pp. 187-188.


Balbi, 2019, p. 188, p. 234.
56 Johnson, 2016, p. 46; Nugroho, 2018. As cited by Johnson, Heghammer’s notion is that a seasoned veteran in terrorist group ranks increases lethality and injury rates.
63 Colgan, Jeffrey D., Petro-Aggression: When Oil Causes War, Cambridge, UK: Cambridge University Press 2013, p. 2.
65 Henderson, 2003, p. 54.


World Tourism Organization (2002), “Tourism Between ‘Moderate Optimism’ and ‘Structural Changes’, WTO Tourism Recovery Committee says,” World Tourism Organization, 21 November, as found in Henderson 2003, pp. 47, 58; Drennan 2007, pp. 158-181. One caveat that some scholars like Drennan point to, are the difficulties of attempts to distinguish between terrorism’s economic effects from broader macro-economic effects.

Balbi, 2019, p. 214.


Hitchcock and Darma Putra 2007, pp. 122-123.

Fall and Epkins 2009, pp. 87-104.


The Straits Times (Singapore) 2002, “Malaysia tourism industry feels Bali blast effect,” The Straits Times (Singapore), 15 November. Available at: https://advance-lexis-com.proxy.lib.wayne.edu/api/document?collection=news&id=urn:contentItem:4782-M1T0-0058-X40M-00000-00&context=1516831; Henderson 2003, p.46, p.57. To be sure, “tourist arrivals” is a measure comparable to “hotel occupancy” — a “tourist arrivals” dip of 28.0% in Malaysia is just under two-thirds of the 43.5% drop in hotel occupancy in Bali reported by Asmarani, 2002.


Ibid., pp. 63, p. 61, pp. 20-21.

Ibid., p. 45,p. 47, pp. 53-57.

Ibid., p. 39.

Balbi, 2019, p. 214.

Ibid.

Nugroho, 2018, p. 131, p. 152.


Johnson, 2016, pp. 56-57.

Ibid., 9

Balbi, 2019, pp. 217, 234, 287.


Johnson, 2016.


Johnson, 2016, pp. 60-61.

Ibid., pp. 58-59.

Asongu and Nwachukwu, 2018.

Ghaderi, Saboori, and Khoshkam, 2017, pp. 558-560. Ghaderi, Saboori, and Khoshkam’s analysis produces a coefficient of -0.041 at the .01 significance level.

Ibid.


Ibid.


Gurtner, 2016; Chasdi, 2014.


Llewellyn, 2021; The Jakarta Post,2020, “Police find thousands of alms boxes allegedly used by Jammah Islamiyah to raise money.” The Jakarta Post, 18, December. Available at:


128 Johnson 2016, p. 52.


133 Schmid, 2013, p. 216.


137 Such as the Asia economic crisis (1997-1998), the Global War on Terrorism (2001- ), the Iraq war (2003), the war in Afghanistan (2001- ), and the SARS virus outbreak (2002-2004)

138 Nugroho 2018pp. 106-107; Hudson 2016, p. 371. Even though advocates of military style counterterrorism approaches point to how terrorism with its political nature differs from organized crime and common criminal activity and thus requires more than policing, the lesson here is that without the subtleties and nuances that many circumstances dictate, military style counterterrorism can be counterproductive.

139 Nugroho, 2018, 160.


143 Huntington, 1968.

144 Waltz, 1959; Nye 1993; Nugroho, 2018, p. 132.


149 Gordon and Lindo 2011.

150 Nugroho 2018 130; Chasdi 2018.


Bibliography


Starr, Harvey and Benjamin Most. 1983. “Contagion and Border Effects on Contemporary African Conflict.” *Comparative Political Studies*, 16 (1), 92-117.


The Straits Times. 2002. “Malaysia tourism industry feels Bali blast effect.” *The Straits Times (Singapore)*, 15 November, Available at: https://advance-lexis-


Chapter 33
Prevention of Revenge Acts and Vigilantism in Response to Acts and Campaigns of Terrorism
Marie Robin

This chapter focuses on the ways in which some people react to terrorism. It first offers a typology of some of the main unlawful reactions to terrorism, classifying them along two axes - the level of violence and the level of organization. Four types of responses are then examined, ranging from non-violent/non-institutionalized reactions to violent/institutionalized reactions. This chapter then focuses on two of these situations - those that involve an actual use of violence - and it examines the dangers posed by revenge and vigilantism at the levels of the state, society and counterterrorism. The chapter concludes by offering recommendations on how to deal with private revenge acts and vigilantism. First, government should ensure that sectors of the population do not feel a need to take the law in their own hands and set up a parallel justice system. Second, leaders of civil society and those holding state power should strive to reduce polarization and inter-community tensions that can lead to scapegoating and new cycles of violence. Third, government should introduce legislation restricting the possession of arms in private hands.

Keywords: prevention, political violence, revenge, terrorism, vigilantism
In the aftermath of a major terrorist attack, and even more so in situations of ongoing terrorist campaigns, some people, driven by passionate anger and grief, take up arms in order to punish the presumed perpetrators or the people associated with them. They do so in order to protect themselves and their core values when the government is perceived as unable or unwilling to act. People take recourse to unlawful actions against terrorism for a variety of reasons, including fear, despair, and a taste for adventure. Feelings of revenge play an important role as these seemingly legitimize the use of force. Terrorist attacks generate both trauma and anger. Members of society often suffer from feelings of helplessness in the face of a hidden or distant perpetrator. Many feel a desire to “do something.” This felt need to do something can sometimes lead ordinary citizens to take up arms to defend themselves, their families and their way of life in a quest to restore normalcy and regain a sense of security. Yet the spontaneous and private recourse to arms in reaction to terrorism oftentimes contributes to a counter-productive escalation of conflict.

This chapter seeks to answer the following research question: Why and how should one prevent the outburst of vengeful reactions and vigilantism in the aftermath of a terrorist attack? It offers a typology of unlawful reactions that might follow a terrorist attack and underlines the dangers of emotional responses to acts of terrorism. It concludes by offering recommendations on how one can prevent the surge of such reactions and thereby reduce the risk of an escalation of conflict.

Theoretical Framework

What exactly do we mean by “vengeful reactions” and what are the types of illegal actions that some individuals and groups tend to take following terrorist attacks? In this section, we offer a typology of unlawful reactions to acts or campaigns of terrorism. This allows us to define revenge acts and vigilantism, and how they sometimes manifest themselves following terrorist attacks.

Why Revenge? Durkheim’s Mechanical Solidarity

Why do some people feel a strong need to react personally to terrorist attacks, even when the victimized people live far away, on the other side of the ocean? What phenomena of identification can explain strong reactions to acts of terrorism?

The Durkheimian notion of “mechanical solidarity” might be helpful to understand the reason why. For 19th century French sociologist Emile Durkheim, mechanical solidarity emerge within a society which is quite homogeneous. In the context of a terrorist attack, feelings of similarity and solidarity emerge from the common experience of trauma and fear as well as the grief that people share. Most importantly, the majority of people identify with the victims, thinking that they could have been one of us, and, as such, most of us feel connected to them by a bond of common vulnerability in the face of sudden unprovoked random attacks. Durkheim attributed “mechanical solidarity” to family ties and kinship. In the age of global mass media, the circle of concerned people is much larger.
Solidarity involves a bond of unity between individuals, united around a common goal or against a common enemy. Identifying the enemy and dealing with the enemy are crucial parts of narratives emerging in the immediate aftermath of a major terrorist attack, sometimes leading to revenge narratives. French sociologist Gérôme Truc studied the societal reactions to terrorist attacks. Using a framework provided by an American colleague, he explains:

“The American sociologist Edward A. Tiryakian has pointed out the way American society reacted to 9/11 is a very clear illustration of the phenomenon that Durkheim portrays in that work under the name ‘mechanical solidarity’. Faced with the attack, Americans more than ever had the feeling of being united. This reaffirmation of national cohesion, an American ‘we’ that for a while took precedence over the singular ‘I’ that compose that community, was particularly reflected in the flourishing, in public space, of a symbol that was, as it were, erected as a totem: the Stars and Stripes.”

In one of his works, Truc studied an initiative taken by the French Mémorial de Caen and the newspaper Ouest-France following 9/11: French people were asked to send letters to Americans. He quoted from one of those letters, which illustrates the link between the feeling of unity, mechanical solidarity, and a desire for revenge.

“It’s the Western world as a whole that is in mourning and our hearts are weeping in unison with our American brothers. We are one family and, together, we will face up to this attack that has killed our people. We weep but we are erect and dignified, and we will stand up to the enemy. We extend our condolences to the American people and share, in its pain, its desire for revenge.”

Revenge feelings, when they surface, emerge from shared grief and a strong identification of the witnesses with the victims. Randall Collins showed how, in the immediate aftermath of an attack, members of the society gather and share their grief, reinforcing the ties that bind them together. Faced with the same trauma, people feel as members of a single aggrieved family, of which one of them was taken away. Research in anthropology has shown how feelings of community/family belonging can lead to feelings of revenge. Evans-Pritchard, in his studies of the Nuer people and the Luo of Kenya, showed how blood ties were systematically mobilized in the context of retributive justice, especially in rituals. A French psychologist, Pascaline Delhaye, also recognized that revenge constitutes one of the two obligations that can emerge from blood ties. To her, family kinship is associated with two natural obligations: the prohibition of killing a member of the family, and the obligation to avenge the murder of one of their own.

Revenge feelings might emerge from the reinforcement of community feelings in the context of strongly felt vulnerability and fear resulting from a terrorist attack. Faced with the atrocity and in order to prevent that terrorist crimes go unpunished, people gather around the victims and their families, determined to punish the perpetrators and avenge the victims - “our brothers and sisters” - for the norm violation.

Nevertheless, ‘mechanical solidarity’ does not automatically lead to revenge. Truc showed that, following 9/11, “nearly 20 per cent of those French women and men who wrote to Americans did so to warn against the evil of taking an ‘eye for an eye’, urging them not to yield to the provocation of terrorists …. The author of one of those letters advised: “As to retaliation, let justice be carried out wisely, without striking innocent civilians.” In the week following 9/11, 76 percent of Europeans expressed a preference for a judicial rather than a military response to the Al-Qaeda’s attacks which killed nearly 3,000 people.
In the context of a terrorist attack, due to the common traumatic experience and to the grief people share, individuals tend to become more similar; there is an increased feeling of community within society. Within homogeneous society, phenomena of “mechanical solidarity” emerge, in which members of a family express the need to protect each other and the need to avenge the offense experienced by one of their own.

Many types of reactions to terrorism can be observed, being different manifestations of “mechanical solidarity.” While some people might express a desire for revenge due to community membership or family kinship, others prefer promoting peace and unity. Before asserting what can be done in order to prevent vengeful reactions, there is a need to properly define what exactly revenge and vigilantism are and how they manifest themselves in the context of a terrorist attack of series of attacks in a terrorist campaign.

**Defining Revenge and Vigilantism**

A basic understanding of revenge refers to a reactive act of punishment that hurts or harms a (member of) a guilty party in retribution for having suffered a wrong or injury. According to one widely used dictionary, revenge is thus the action “to inflict injury in return for.”\(^{17}\) Several characteristics can be associated with revenge: the use of violence (or the threatened use of violence); the perception of a preceding wrongdoing; its appearance within a close-knit community; and a certain satisfaction resulting from harming the other.\(^ {18}\)

Although the notion of revenge is traditionally associated with strong emotions and passions, vengeance can also be understood as a strategy. Thanks to its duality – as both a vice and a virtue\(^ {19}\) – vengeance also features prominently in the vocabulary of terrorists. Martha Crenshaw noted that “one of the strongest motivations behind terrorism is vengeance, particularly the desire to avenge not oneself but others.”\(^ {20}\) In recent years, several ISIS’s attacks were ‘justified’ as a “Vengeance for Sham.”\(^ {21}\) Similarly, Brenton Tarrant, the mosque attacker in Christchurch (New Zealand), referred in a manifesto to his desire to “take revenge for the thousands of European lives lost to terror attacks throughout European lands.”\(^ {22}\)

In January 2015, the Kouachi Brothers, right after committing their deadly attacks on the offices of Charlie Hebdo in Paris shouted in the streets of Paris: “We avenged the Prophet.”\(^ {23}\) Vengeance narratives were also widely used by the Front de Libération Nationale (FLN) and the Groupe Islamique Armé (GIA) in Algeria in their attacks against the government.\(^ {24}\) The Provisional Irish Republican Army (IRA) also often sought revenge for what it called the crimes committed by the English crown.\(^ {25}\) Already in 1878 in Russia, Vera Zasulich\(^ {26}\) had portrayed her assassination attempt on the governor of Petersburg as an act of rightful vengeance. Thus, vengeance constitutes a powerful motivation for terrorism, making it also a mobilization tool for terrorist organizations looking for new members.

Attributing vengeance motives solely to the terrorist side would nevertheless prove highly misleading. Indeed, revenge can be observed on both sides in a conflict dyad. Terrorist attacks generate shock, anger, and fear among a society under attack and beyond that within the international community as a whole among all those who identify with the victims and not with the goals or methods of the terrorists. In some cases, those aggrieved by a terrorist attack might actually take - or threaten to take - up arms against those deemed responsible. Their desire for vengeance can, however, lead to additional acts of violence – creating a spiral of violence with tit-for-tat (re-)actions escalating the conflict.

Vigilantism overlaps with revenge in several ways. The British criminologist Les Johnston defined vigilantism as “a social movement composed of voluntary private agents who, on the basis of a premeditation and faced with what they perceive to be a transgression of institutional norms, wish to control criminality and guarantee the security of the members of their movement by using or threatening to use violence.”\(^ {27}\) Like revenge, vigilantism involves a form of violence, initiated in response to what is perceived to be an offense (against individuals,
society, community values etc.). Vigilantism, like revenge, is also deeply tied to one’s definition of a community and the perceived limits of the in- and out-groups. Although Johnston’s definition has become widely accepted, it somehow disregards the occasionally ambiguous position that the state might take vis-à-vis vigilante movements. Those holding the reigns of the state can indeed find common interests with vigilante movements and, to some extent, accommodate and use these, leading to a complementary but problematic division of labor in exercising law and order functions. 

Vigilantism, like vengeance, is an ambivalent notion. William Safire, a famous New York Times journalist, identified two opposite meanings:

“One is positive (to impose the law where it is missing) and the other is negative (to take the law into his own hands). When one uses the notion today, in an historical understanding, it refers to rough justice on the border rather than the repression of Black people on the South, and this is rather a compliment. But when it is employed to refer to contemporary practices, the vigilante notion – and even more its associated -ism – generally serves to suggest outdated and undesired methods, in a pejorative sense.”

According to Gilles Favarel-Garrigues and Laurent Gayer, practices of vigilantism emerge from two types of motives: a willingness to restore order, acknowledging what people deem to be the essential values of their society, and a desire for justice. On the one hand, vigilantes want to prevent new attacks by protecting those they deem to be their fellow citizens. On the other hand, vigilantes wish to punish those whom they hold responsible for crimes to avenge the victims and the aggrieved society. Depending on the cases or contexts, one motivation or the other can dominate, leading to different reactions to the initial attack.

A Typology of Reactions to Terrorism
Reacting illegally to terrorism first requires identifying a target – i.e. someone deemed responsible for the initial offense and whose wrong deeds call for a response. In this paper, we consider that the choice of targets of avengers and vigilantes follow a rational choice process with priority being given to:

1. The terrorists themselves (provided that they are still alive).

In case they are out of reach, the avengers and vigilantes will seek to target:

2. The direct accomplices, or members of the terrorist group; and finally
3. Those deemed to be associated with the terrorists due to their nationality, religion, community, following a sense of “shared accountability” along – more often than not – racist and/or xenophobic lines.

For the general preventing purpose of this chapter, we thus posit that the avengers’ preferences will follow this three-step preference ordering. Based on this first assessment, vigilantism can then be classified in terms of the degree of violence or in terms of the degree of organization.

Degree of Violence
Most reactions to terrorism do not involve the use of private violence and remain within the realm of the rule of law, at least in democratic states. French scholars Gérôme Truc, Christian Le Bart and Emilie Née explored the various expressions of unity that emerged in narratives
in the immediate aftermath of an attack. Jack Santino and Erika Doss, on the other hand, focused on ephemeral shrines and memorials, showing how emotions were publicly expressed in the aftermath of an attack. They all find that media and political leaders usually display a narrative revolving around the notions of unity and community belonging, just like the common people who gather in public places and show their emotions. The standard narrative includes notions like “they won’t destroy us, together, we are stronger.” Following the fateful 9/11 attacks perpetrated by Al-Qaeda and the massacre carried out on 13 November 2015 in Paris by followers of ISIS, thousands of manifestations of support for the victims and their families could be seen. These lawful reactions to terrorism are not the focus of this chapter; rather it analyzes the illegal behaviors that follow some terrorist attacks.

Among the manifestations of remembrance and sorrow, some people feel a need to display more extreme behaviors, outside the realm of the rule of law. Unlawful reactions can be classified according to the level of violence involved.

Illegal reactions to terrorism can involve violence, such as attacks on members of a ‘suspect community’, or counter-violence against presumed accomplices of the original perpetrators. At the far end of the axis, are death squads engaging in extra-judicial killings, which are designed to punish perpetrators and avenge victims. One practice of paramilitary groups is the lynching of people right- or wrongfully associated in some ways with the terrorists.34

However, often the display of arms is enough. Thus, in their edited volume on vigilantism against minorities and migrants, Tore Bjørgo and Miroslav Mareš found that:

> “Most vigilante groups do not actually carry out acts of violence. However, they do usually display a violent capacity through a performance of force, whether they parade as a paramilitary militia (with or without weapons) or patrol the streets in groups dressed up with group symbols or uniforms. Their display of force is obviously intended to have an intimidating and deterring impact on their designated target groups (…) as well as political opponents.”35

On the low- and no-violence side of vigilantism, one can find activities like computer hacking, naming and shaming, public humiliation, online collective mock trials or the burning of flags.

**Degree of Organization**

Reactions can also be classified according to the level of institutionalization required. Reactions to terrorism can occur within pre-existing organizations or emerge spontaneously from crowd (re-)actions. Angry individuals - lone wolves - can also carry out such actions. Researching vigilantist practices in general, Fourchard found:

> “At one side of the spectrum are structured organizations (criminal organizations or unions) which, for different reasons were able to - or had to - integrate police functions to their activities (…). On the other side are groups of individuals who assume police roles without seeming to do so. (…) These are the informal groups of sociability which surveil certain neighborhoods, such as the fada in Niamey or the groups of youth in the popular neighborhoods of Nairobi.”36

Therefore, on the “spontaneous” side of the axis we find the perpetrator of the Christchurch attack against two mosques in 2019, qualified by some as “lone wolf” actions, “justified,” by the perpetrator, as punishments to avenge the deaths of Europeans by the hand of Muslims during recent terrorist attacks. At the “institutionalized” side of the axis are practices
implemented by quasi-state organizations, which have emblems, flags and uniforms and act as a substitute for the state in assuming police functions. Bjørgo and Mareš, describing paramilitary militia movements, stress the high degree of institutionalization of these groups: “What distinguishes these militias from other forms of vigilante groups is that they are modelled on a military style and form of organization.”37 Their members wear uniforms, perform parades and marches; a structured chain of command and military skills are visible.

Classifying Reactions

Dividing the field of vigilante action along an axis of violence and one of institutionalization, one gets four different types of illegal reactions.

1. A Need to “Do Something”: Non-violent and Non-institutionalized Reactions to Terrorism

In this case, reactions are spontaneous. Out of mechanical solidarity, members of society who share trauma and grief want to do something. Actions in this category do not involve the use of violence. Rather, persons belonging to this category engage in, for instance, cyber operations in order to identify the potential accomplices of the terrorists. Such operations emerge from individual initiatives; they stem from a personal willingness to “do something,” while still staying within the rule of law. Actions by cyber activists can include identification of extremist social media accounts, surveillance of online tortious activities, hacking, suppression of content, naming and shaming, as well as social media squads chasing down suspects on the Web, and collective online trials in which so-called Internauts can vote on the best sanction to be applied for alleged terrorists and accomplices.

In situation 1, individuals offer their skills and time in order to combat terrorist groups in general. Such ‘combat’ occurs on the virtual stage, targeting reputation and prestige. However, it usually does not involve the use of violence, just like situation 2.

The Anonymous Network’s Fight against ISIS

The Anonymous network gathers individuals with IT skills in order to hack public institutions, private companies and denounce corrupted leaders. Created in 2003-2004 in the framework of the 4Chan forum, the network gathers individuals with a wide variety of profiles, motives and skills, making it a nebulous object for study. In the context of the fight against the Islamic State, the network contributed to weakening the terrorist organization through the hacking of various pro-ISIS social media accounts etc.

In April 2015, “over one hundred hackers helped to compile and release a list of thousands of Twitter account names as part of #OpISIS, a campaign to disrupt the Islamic State’s virtual presence.”38 Some key influencers emerged in the online fight against the group. Thus, the website Xrsone.com organized the different vigilante efforts, by gathering media mentions, target lists and pro-ISIS account lists. Activists’ accounts include @CtrlSec as well as @Iridium_Black which regularly tweet the names of pro-ISIS accounts, asking other internauts to get mobilized so as to persuade Twitter to remove them from the platform.39 In France, internauts on Twitter, gathered under the name Katiba des Narvalos, also track down pro-ISIS accounts.40

Benjamin Loveluck analyzed this online form of vigilantism: “The goal is not only to alert authorities or the public opinion but also to ‘make justice’ by engaging in active forms of
surveillance or targeted deterrence, especially through an increased unsolicited attention or negative publicity.”

The Anonymous network succeeded in taking down numerous Twitter accounts and Facebook pages linked to the terrorist group ISIS. In a statement released in 2015, the network explains: “The terrorists that are calling themselves Islamic State (ISIS) are not Muslims! (…) We will hunt you, take down your sites, accounts, emails, and expose you. From now on, no safe place for you online. You will be treated like a virus, and we are the cure.”

Other online activities emerged in order to counter terrorism. Thus, following the 2013 Boston Marathon bombing, members of the Reddit forum contributed to spreading the call for witnesses sent by the FBI by creating a section (subreddit) dedicated to the identification of suspects. This initiative was initially praised as an innovative form of “collective intelligence.” However, it quickly turned into a fiasco with the scapegoating of an innocent student, Sunil Tripathi, who was left alone to face popular vindictiveness.

Steve T. Zech examined the pros and cons of Anonymous network’s contribution to the fight against the so-called Islamic State. As illustrated in Sunil Tripathi’s case, the involvement of numerous private citizens in the fight against terrorism can lead to tragedies. However, scholars have shown that Anonymous and other cyber activists can prove beneficial in the fight against terrorist groups in that they seem to succeed in limiting ISIS’ ability to spread its ideology and vision. In an article released in Foreign Policy, Emerson Brooking argued that the US should support the Anonymous affiliates already combating the Islamic State by putting them on the government payroll or by offering Bitcoin bounties. However, several challenges are posed by the Anonymous participation in the fight against the terrorist organization. First, according to Steven T. Zech, Anonymous activities are not subjected to any mechanism ensuring accountability. As such, in the absence of cooperation with the intelligence community, Anonymous members might actually harm the fight against terrorism without bearing clear responsibility. Second, tolerating the involvement of Anonymous cyber activists in the fight against ISIS amounts to approving “direct civilian participation in combat operations,” which raises issues in terms of International Humanitarian Law as to the status of such combatants as well as their responsibility and protection status.

2. A Need to “Prevent other Attacks and Protect our Society”: Non-violent and Institutionalized Reactions to Terrorism

The restoration of order is one of the two main motives triggering vigilante practices, according to Favarel-Garrigues and Gayer. Faced with vulnerability and impunity, order-motivated vigilantes wish to ensure the security of those they define as their fellow citizens and seek to prevent the occurrence of new attacks. To do so, these groups take upon themselves police functions, including surveillance, patrolling and/or law enforcement.

To be able to replace the state’s police as law enforcement operators, these groups are generally institutionalized. They exhibit discipline, hierarchical patterns, and sometimes display uniforms, as do, for instance, members of the Extreme Right vigilante group Forza Nuova operating security walks in Italy. Although these groups possess capabilities to use force, they generally do not use them. Thus, although members of Génération Identitaire sometimes carry arms, they rarely actually use them.

These groups identify where the priorities and threats are in order to implement their own vision of security, defining the border lines between in-group and out-group. Targeting certain segments of population indeed contributes to defining who the enemy is, thereby redefining the community, and exposing divisions within society. In section two of this chapter, we examine the potential implications of such divisions of the national community.
Examples of practices include surveillance of neighborhoods, patrols, intelligence gathering, but also structured online platforms. Historical examples of vigilantism generally took this form, with armed formations patrolling the streets. Such was the case of Jewish vigilantes in the West Bank, or the street patrolling groups like the Soldiers of Odin, operating in Finland, Norway and Canada.

---

<table>
<thead>
<tr>
<th>Patrolling European Borders: the Example of the Far-right Extremist Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Génération Identitaire is a French extreme-right group which was created in 2012 as heir of the extreme-right groups “Jeunesses Identitaires” (2002) and “Une autre jeunesse” (2009). The group is mostly known for its occupation of the construction work site of a mosque in Poitiers on 20 October 2012. Following this occupation, seven persons were incarcerated for material damage, the organization of a public gathering without authorization, and complicity in inciting racial hatred. In April 2018, members of the group stood on the French-Italian frontier in order to spot asylum seekers trying to cross the border. Their goal was to prevent the migrants from entering the country. Without actually carrying weapons or using violence, the members of the group tried to discourage asylum seekers by carrying placards saying: “Closed border. Europe will never be your home. That is out of question. Go back home.” Leaders of the group faced up to six months of jail time and a 75,000 euros fine. The Génération Identitaire movement is highly institutionalized. The group owns a flag – an inspiration from the lambda of the Spartans -, a clear process of membership selection, as well as an established hierarchy. They sometimes wear uniforms. The group has never been convicted for acts of violence. During court trials, members of the movement faced charges of material damages and incitement to hatred but none of them was indicted for violence. Thus, in the French Alps, the group tried to stop the asylum seekers by forming a human chain at the border in order to prevent them from crossing. The group is overtly xenophobic and opposed to the arrival of Muslims in Europe. It attributes terrorist attacks occurring in Europe to the arrival of African and Arab immigrants in Europe. Although the movement is not affiliated with any political party, their ideas are close to those of Hungarian President Victor Orban, former Italian Ministry of Interior, Matteo Salvini, and French politician and European MP, Marine Le Pen.</td>
</tr>
</tbody>
</table>

Border patrolling groups resemble the traditional image of vigilantes. Although they are generally not using violence and simply display their capacity to use force, these groups can sometimes become violent in case of resistance. Most of all, vigilant groups obeying to this model seek to restore their own version of order to prevent new attacks from happening, targeting, to this end, certain segments of the population that they hold responsible for certain crimes. Non-violent and institutionalized vigilante groups mostly take on police functions, thereby seeking to replace the government as the main law enforcement instrument. Consequently, these groups threaten the state politically by challenging the state’s monopoly of the legitimate use of force.

3. A Need to “Punish them”: Violent and Non-institutionalized Reactions

Certain acts of terrorism are often hard to understand; their apparent arbitrariness can trigger rage and anger among the population, or sectors thereof. Aroused passions drive some people to take up arms and engage in ‘rough justice’. British philosopher David Hume examined the role of “hot passions”. In his Dissertation on Passions, Hume showed how anger and revenge
trigger a mechanism (casuistic) that almost inevitably leads to actual violence. Revenge is about action. Outbursts of rage easily turn to violence although they are mostly unorganized and spontaneous. Passionate reactions can be either individual or collective but, in the end, they rarely lead to a structured organization with planning, preparation and discipline. Outbursts, by definition, imply a form of spontaneity and are of short duration. Examples of practices include the burning of places of worship, lynching, and certain forms of lone wolf (re-)active terrorism. The case of the Christchurch shootings is interesting in this respect.

### Avenging European Deaths in New Zealand: the Case of the Christchurch Shootings

On 15 March 2019, a white supremacist terrorist from Australia attacked two mosques in Christchurch, New Zealand, killing 51 people and injuring 49 others. The perpetrator streamed the attacks live in real time on Facebook. Known for his extremist far-right ideas and his sympathy for white supremacist groups, Brenton Tarrant (28) was arrested and charged with murder. For his attack, he had no known accomplices from organized far-right groups and/or terrorist groups.

The terrorist’s 74-page manifesto “The Great Replacement” clearly refers to several conspiracy theories, including the white genocide theory. He explains how he started thinking about such an attack two years in advance, in reaction to jihadist terrorist attacks against Western countries, especially in Europe. His motives stemmed from anti-immigration sentiments and hatred against Muslims. He claimed he had to “take revenge for the thousands of European lives lost to terror attacks throughout European lands.”

Needless to say, the Muslim victims in New Zealand had nothing to do with victims of Islamist terrorism in Europe - but in the twisted mind of this terrorist such a link had been made. The attacks were non-institutionalized. Brenton Tarrant was a lone actor, not affiliated to any specific group. He even explained, in his manifesto, that he did not belong to a Nazi organization.

Reactive terrorism is nothing new but has seen a worrisome increase in recent years. Such reactive terrorism often leads to an escalation of conflict. In the days following the Christchurch attacks, hundreds of ISIS Telegram posts claimed revenge for “our Muslim brothers killed in New Zealand.”

### 4. A Need to “Avenge the Victims”: Violent and Institutionalized Reactions

This case is of special interest in the framework of prevention research. In the immediate aftermath of terrorist attacks by non-state actors, some enraged people get together and form paramilitary units in order to avenge the victims. A clear example of such reactions can be found in Nigeria’s C-JTF.

### Civilian Vigilantes in Nigeria (C-JTF): Between Personal Revenge and Political Instrumentalization

In Nigeria, young people joined the paramilitary Civilian Joint Task Force (C-JTF) in order to “bring justice” to victims of Boko Haram.

In June 2013, in a context marked by regular violent attacks by the armed troops of Boko Haram, hundreds of civilians from the Borno state of Nigeria (in the north of the country where Boko Haram fighters were, and are, particularly active) were gathered in a vigilante organization, known as the Civilian Joint Task Force (C-JTF). The C-JTF is designed to prevent further Boko Haram attacks and to ensure law enforcement in Borno State.
creation of the C-JTF came just one month after the declaration of a state of emergency by Nigerian President Goodluck Jonathan. Members of the vigilante C-JTF included mostly urban youth, most of them teenagers. The leader of the group, Baba Lawal Ja’afar from Maiduguri, was 30 years old in 2013. C-JTF members wear uniforms, are embedded in a chain of command, and have a degree of discipline. They also assume police functions and overtly use force. Several mass executions have been attributed to this vigilante group. Jean-Philippe Rémy, a journalist for Le Monde, quoted a source saying “The C-JTF considers that if a village refuses to create its group of militiamen, they are part of Boko Haram, and thereby, a legitimate target.”

Out of the 26,000 members of C-JTF, less than 1,800 receive a salary, an indication that the motivation for involvement lies elsewhere. Recruitment in the C-JTF resulted from two main motives, according to Thurston. First, personal reasons led some Nigerian youth to join the vigilante group. One young man explained: “I joined the voluntary vigilante group to make sure that all the people feeding and aiding Boko Haram were severely dealt with. I want to see them arrested, captured, and made to face trial for their atrocities. It will mean a great deal of happiness and satisfaction to me because I have lost friends and persons close to me.” Second, civilians joined the vigilante group in order to counter Boko Haram’s repeated destructions of schools.

Some observers have argued that the C-JTF was a big success, both for president Goodluck Jonathan and for Nigeria. Indeed, by June 2013, vigilantes had expelled most of Boko Haram’s fighters from the city of Maiduguri. These successes were made possible thanks to the C-JTF local knowledge of the territory and the ability of its members to identify Boko Haram members by name.

Several concerns arise from the involvement of civilians in the fight against Boko Haram in Nigeria. It increased the interpersonal dimension of the conflict, leading neighbors and family members to fight against each other in the streets of Maiduguri. The interpersonal dimension of the conflict increased suspicions of treason, leading to harsh reprisals and bloody revenges. Second, the involvement of civilians is problematic in terms of government responsibility. Some have argued that the C-JTF was born out of a civilian desire to fight against jihadists. Other have argued that the group was a brainchild of president Goodluck Jonathan and the Nigerian military. Indeed, according to Thurston, there were reports of Borno residents being conscripted into C-JTF units as well as signs of a clear backing of C-JTF operations by Borno State’s authorities. In September 2013, the government initiated the Borno Youth Empowerment Scheme which offered weapons training to more than six hundred vigilantes. By late 2013, more than 1,800 vigilantes were officially under the local government’s authority, receiving a monthly salary of $100 USD.

The involvement of the C-JTF also contributed to the escalation of the conflict. Although the state government did not formally arm all vigilantes, the C-JTF carried out several violent actions. Following Boko Haram’s prison break in Giwa in March 2014 that freed many prisoners, the C-JTF carried out punitive operations. As reported by Amnesty International: “As the military regained control, more than 600 people, mostly unarmed recaptured detainees, were extra-judicially executed in various locations across Maiduguri …. Eyewitnesses in Jidari Polo, also in Maiduguri, described how members of the “Civilian Joint Task Force” rounded up freed prisoners and handed them to soldiers. More than 190 people were executed, many of whom were too frail to run.”

According to Thurston, the C-JTF also lynched several Boko Haram members, even when the security forces objected to the practices. In Nigeria, the involvement of civilians of the C-JTF – either voluntarily or ordered by president Goodluck Jonathan – led to an escalation of the conflict as multiple cyclical reprisals occurred at the local level between neighbors, leading to mass lynching, death squads and punitive forms of justice.
The IRA and Sinn Féin: Paramilitary Vigilantism in Northern Ireland

Andrew Silke explored the relationship between the IRA, Sinn Féin and paramilitary vigilantism in Northern Ireland. The IRA and Sinn Féin have taken on police activities since the beginning of their fight. The Provisional IRA thus started off its violent activities by killing two local gangsters. The groups regularly carried out “punishment attacks,” according to Silke. When the government carried out raids and arrests, militant Republicans responded by attacks of their own, designed to avenge their arrested comrades. Punishment attacks also targeted local criminals who were not respecting the values of the society. “The violence of many so-called ‘punishment attacks’ can be extreme, and a number of people have died as a result of injuries that were intended to be non-fatal.”

Adding to its policing activities, Provisionals also wants to ensure the “administration of an informal justice system.” Their policy to implement an alternative justice system led to many casualties. According to Silke, “in total around 40,000 people were estimated to have been physically injured as a result of political violence in Northern Ireland, indicating that vigilantism accounts for around 10 percent of the conflict’s [total] non-fatal casualties.”

Examples of planned reactions to terrorism out of revenge include the formation of paramilitary militias, death squads and organized lynching. Such reactions amount to vengeance and ‘justice’-driven vigilantism.

Cases of violent and institutionalized violence generally involve paramilitary groups engaged in collective lynching, death squad activities and mutilations like, in the case of Northern Ireland, ‘knee-capping’. These manifestations are especially problematic in that they reflect a level of planning and organization that go beyond simple passionate responses. They can have social, political, military and normative consequences for the society and the state as a whole.

In this section, we identified four different types of illegal reactions to terrorism. Situations 1 and 2, in that they are not involving direct violence, are of less interest for the following sections in which the dangers posed by such reactive manifestations of violence are discussed.

Why Should One Prevent Revenge Acts and Vigilantism?

In the following, the focus is on situations 3 and 4, i.e., violent and non-institutionalized reactions, and violent and institutionalized reactions. Situation 3 relates to personal forms of vengeance, outbursts of passion that tend to provoke further violence. Situation 4 corresponds to immediate justice-seeking vigilantism and group vengeance, by means of organized direct action in order to avenge the victims of terrorism. Indeed, situations 3 and 4, in addition to threatening the governance of the state and social cohesion, tend to lead to further violence, thereby leading to a new spiral of violence.

In this section, we will identify the four main reasons why revenge acts and immediate justice-seeking vigilantism ought to be prevented.

Reason 1: Revenge usually does not work

Revenge acts and vigilantism do usually not succeed in achieving their objectives. The main objectives behind the reactions described above are threefold: to punish the offender, to satisfy the victim, and to protect the society from further attack. We shall assess the efficacy of revenge and vigilantism in achieving each of these three goals. Avengers and vigilantes seek to punish
those they deem guilty of the terrorist offense. The theory of utilitarianism, developed in the early 19th century, identified the main purposes of criminal punishment. By punishing a criminal, the purpose is to bring about positive outcomes. Three objectives are to be identified:

1. Rehabilitating the criminal and ensuring that he will not commit any more crimes.
2. Deterring the criminal (specific deterrence) and others (general deterrence) from undertaking similar illegal activities, and
3. Incapacitating (through prison sentence) the criminal in order to protect the society and the state while he is in prison. Eisenstat shows that, following the utilitarian theory, only if punishment furthers these objectives, punishment is warranted.69

Revenge, as a form of punishment, rarely succeeds in achieving these goals, especially in a context of terrorism. While it can be argued that some revenge acts and vigilantism can achieve objective 3, leading to the incapacitation of the criminal, it usually does not succeed in achieving objectives 1 and 2.

Objective 1 refers to the rehabilitation of the criminal. Hegel highlighted how vengeance only calls for new vengeance.70 Undertaking an act of violence against the terrorist will only marginalize him even more and feed a new desire for revenge against those who injured him.71 By promoting violence, revenge does not promote rehabilitation.

Objective 2 refers to deterrence. In a thought-provoking article on counterterrorism, Tore Bjørgo, speaking about military retaliation, noted that:

“Military reprisals after terrorist attacks have also been very popular with the general public of countries such as the USA and Israel because they portray an image of the authorities and politicians taking action and not being cowed by terrorists. Herein also lies a great temptation to resort to punishment strikes even if it is doubtful that they will have a deterrent effect.”72

At the local level, punishment operations against those people deemed to be responsible for terrorist crimes are unlikely to have a deterrent effect.73 Revenge does not allow a rehabilitation of the criminal, nor does it appear to have a major deterrent effect on potential new recruits wishing to join a terrorist group.

However, this conclusion is insufficient to qualify revenge as useless. Revenge is linked to the presumed needs of the initial victim or those close to the victim. Revenge is thus victim oriented. Gollwitzer and his colleagues have shown that revenge brings satisfaction to the avenger, who experiences satisfaction when the offender understands revenge as a punishment for an act of violence.74 In addition, avengers also undertake revenge in order to find some form of closure. While the original offender often remains unpunished, the avenger will find somebody associated with the original perpetrator.75

Does revenge bring closure to the immediate victims (if they survive a terrorist attack)? Reactions to terrorism have shown that direct victims of the attacks not infrequently call for peace and justice (within the framework of rule of law).76 One victim of terrorism interviewed explained to this author:

“There are two ways to respond to a jihadist terrorist attack. The first one is to consider that Islam is responsible for my injuries. Therefore, I hate Islam. The second option is to consider that it was hatred and intolerance that hurt me. Therefore, what I hate, is hatred. Direct victims usually go the second way and they choose to fight hatred and promote tolerance.”77
In a remarkable book, French writer Antoine Leiris, who lost his wife in the ISIS attack on the Bataclan concert hall in Paris in November 2015, described how he refused to offer his hatred to the terrorists. Revenge, because it leads to new hatred and violence, usually does not succeed in bringing closure to the direct victims of terrorism.

A third objective of revenge act and vigilantism is to protect the society from further wrong deeds. This protection includes incapacitating current terrorists through the use of violence; but also, more indirectly, preventing the emergence of new terrorists by providing – paradoxically - a sense of justice and law through their vigilante activities. Patrols and law enforcement activities by private groups, corresponding to situations (II) and (IV) serve particularly this goal.

In this case, studies have shown that vigilantism might “work” in that it offers some protection against attack and a form of stability, especially where states are unable or unwilling to do so. Thus, in Nigeria, the C-JTF, through the use of force, was able to effectively counter some Boko Haram fighters and activities, resulting in a severe loss of territory by the terrorist group and a reduction of attacks against citizens in the Borno State. Vigilante activities may help to prevent new attacks by the display or use of force.

In addition, like police forces, vigilantes can contribute to spreading ideas of justice and respect of the law (in spite of being illegal itself) in areas where the state authorities do not seem to do so. Researching the case of Bolivia, Daniel M. Goldstein has shown that:

“Such acts (are) a form of political expression for people without access to formal legal venues, a critique of the democratic state and its claim to a rule of law. Through such violent practices, the politically marginalized find an avenue for the communication of grievances against the inadequacies of the state’s official legal order, while at the same time deploying the rhetoric of justice and law to police their communities against crime.”

Vigilantism offers a specific hierarchy of norms, between those who have to be defended at any cost and those whose transgression is made necessary by the legitimacy of the cause (in the eyes of the perpetrators). In addition to threatening the state’s monopoly of force, revenge and vigilantism fundamentally question the hierarchy of norms within the society. Lastly,
revenge and vigilantism, challenge the authority of the state and its capacity to enforce punishments. By definition, the operations under examination here are illegal. Consequently, they require an additional intervention of the state in order to punish the criminal perpetrators. However, in reality, some states actually tolerate, or even encourage vigilante groups to perform police functions. As indicated in a box earlier in this chapter, in Nigeria, the C-JTF has close ties with the local state authorities and might in fact have been the result of a government initiative in order to combat Boko Haram in Borno State. Steven T. Zech, who worked on the Anonymous network’s contribution to the fight against ISIS, noted: “Cases of direct civilian participation in combat operations have raised important questions about the legality and desirability of involving non-state actors in violent conflict.”87 Two questions stand out regarding the status of vigilantes: Are they combatants or civilians? and, in case of humanitarian law and human rights abuses, who is to be held responsible, the vigilantes or government backing them?

Reason 3: Revenge Weakens the Norms of Society

Revenge and vigilantism do not only threaten the authority of the state; they also contribute to weakening essential features of society – both socially and normatively. Revenge first threatens the society itself by increasing inter-communal tensions and divisions within the society. Revenge needs an enemy. When those direct responsible for a terrorist attack cannot be found (e.g., in the case of suicide terrorism or when the perpetrator manages to escape the scene of crime), avengers search for other targets (e.g., presumed accomplices). René Girard documented the phenomena of scapegoating that can lead an entire society to arbitrarily designate one person as the responsible for the crimes committed against the group.88 The scapegoat then suffers for others, sometimes resulting in his death. The designation of a scapegoat usually follows the lines of inter-community tensions. A recent example of this could be found in Sri Lanka. The Easter Sunday attacks of 21 April 2019, targeted three churches and three luxury hotels in a series of coordinated terrorist suicide bombings, resulting in 259 deaths and more than 500 people injured. Following those tragic attacks, hostility against the Muslim community increased significantly in Sri Lanka:

“In the city of Negombo, where over 100 people were killed at the St. Sebastian’s Church during Easter prayers, many Pakistani refugees said they fled after threats of revenge from locals. Now, anger against Muslims seems to be spreading. On Sunday, a violent clash erupted between local Muslims and Christians after a traffic dispute. “The suspicion towards them (Muslims) can grow and there can be localized attacks,” said Jehan Perera of a non-partisan advocacy group, the National Peace Council. “That would be the danger.” A ban on facial veils and house-to-house searches by security forces in Muslim-majority neighborhoods across the country have added to the distrust.” Consequently, since “successive Sri Lankan governments had failed to address what he called a rise in Islamic extremism, Sri Lankans might be forced to do it on their own.”89

In Sri Lanka and elsewhere, revenge and inter-community tensions feed each other in a vicious circle than tends to generate more hatred and further violence. A second societal threat posed by acts of revenge and the formation of vigilante groups can be found in the normative consequences for the community. The use of private violence in reaction to terrorism challenges the existing authority and societal norms.
Reason 4: Revenge is often Counter-productive in the Fight against Terrorism

It can be argued that revenge and vigilantism, rather than deterring future terrorists, actually increase the pool of new recruits, thereby reinforcing terrorist groups and their cause. It is well known that many terrorist groups seek, by their actions, to provoke reactions that can increase internal divides in society and generate increased social tensions. Provoking an over-reaction can bring new recruits to the terrorist cause and, in the end, produce more terrorism.

René Girard theorized this phenomenon as an *escalation to extremes*: violent challenges call for stronger responses to outmatch the enemy’s violence, leading to a spiral of violence. Tore Bjørgo also noted that,

> “Several studies have shown that such reprisals do not lead to a reduction in the number of acts of terrorism, rather they result in an escalation in terror activities (…) Revenge and reprisals are one of the key driving forces behind terrorism. They are also one of the driving forces behind states’ retaliations for acts of terrorism. Provoking the state into overreacting is one of the classic terrorist strategies.”

Another author, John Quigley, found in his research that “Efforts against terrorism do not justify the lawlessness represented by forcible abduction. Vigilantism is no solution to terrorism. It engenders only further lawlessness.”

How Should One Prevent Revenge Acts and Vigilantism?

This section seeks to explore how one could prevent revenge acts and vigilantism in response to terrorist acts and campaigns. In order to answer this question, one has to look at the risk factors behind revenge acts and vigilantism and how these can be prevented from occurring. Tore Bjørgo and Miroslav Mareš have studied manifestations of vigilantism against minorities and migrants. They identified nine (risk) factors which contribute to the emergence of vigilante groups:

1. A widespread perception of crises and threat to our society and lifestyle.
2. The threat of crime is identified with specific groups that become objects of hatred and fear.
3. Specific shocking events causing moral panic trigger vigilante activities.
4. The perception that the police and other authorities are either unable or unwilling to protect the citizens from threats to their safety.
5. Lack of trust in governmental institutions.
6. Countries with a permissive legislation for armed self-defense or civil patrols provide opportunities for vigilantism.
7. Traditions of vigilantism and militias.
8. [Existence of] a base of support of vigilantism among the public and among political parties.
9. When the police and other authorities turn a blind eye to vigilante violence.

Subsequently, Bjørgo and Mareš identified some of the factors that can contribute to a decline of vigilantism:

1. When the perceived threat is reduced or appears less acute.
2. When the police and other authorities are able to demonstrate that they are in control of the situation.
3. Level of trust in the police and other authorities.
4. Lack of support for vigilante groups and activities from the public, politicians or the news media.
5. When the police and other authorities strike down hard on vigilante violence and hate crime.
6. Restrictive legislation on vigilantism and police enforcement of such laws.
7. The inherent tendency in extreme-right movements towards internal conflicts and splits.  

In the specific context of terrorism, three categories of measures can be taken in order to prevent (or at least reduce) revenge acts and vigilantism following terrorist acts and campaigns:

1. Fight the need;
2. Fight the divisions, and
3. Fight the means.

**Fight the Need**

Both revenge acts and vigilantism belong to the realm of private justice, with certain individuals feeling the need to apply their own form of ‘justice’ in order to punish the group of people deemed responsible for the victimization that has occurred. In order to prevent such non-state forms of justice, institutional official forms of justice need to be strengthened. Preventing vigilantism and revenge acts requires an increase in the level of trust of people in the police and in other state authorities. For that, it is necessary that these actors are clearly in control of the situation. Revenge and vigilantism arise because of a popular mistrust in the ability of law enforcement to sanction those responsible for acts of terrorism. Bjørgo and Mareš noted, in the context of migration control:

“A common feature of all these vigilante border patrols is that … they make an effort to demonstrate the willingness of vigilantes to protect their “own country” in the case of worse migration flows and they want to demonstrate that the government is not able to do “its best” against migration. It is mainly a media strategy to affect the broader public and win “hearts and minds” of people for ideas which vigilantes represent – including undermining the legitimacy of the political regime.”

Ultimately, measures from this category mostly fall onto the State’s shoulders - including its police forces, secret services and military - in that it is the government authorities that need to be seen as willing and able to act, thereby discouraging private policing initiatives.

Prevention of revenge acts and vigilantism following a terrorist attack or campaign should thus include the following measures in order to fight the urge some people feel to take the law into their own hands:

1. The state should make sure to present an accurate evaluation of the actual threat. Indeed, an over-estimation could increase the perception of the threat, thereby making the direct intervention of the members of the public even more necessary in order to counter it; an under-estimation could damage the trust of the population in the authorities, feeding conspiracy theories and mistrust.
2. Offering transparency about the actions taken by the state and its security forces in order to show what is actually being done to combat terrorism. Showing that the state takes all necessary measures in order to combat terrorism both inside and outside the
national territory will correct the misconception that the government is unable or unwilling to take action in order to deter or neutralize further terrorist attacks. In implementing such measures, those holding state power should make sure to remain within the realm of the rule of law.

3. *Rebuilding trust between state and society* by eliminating stigmatization of, and confrontations with entire segments of the population – the ‘suspect community’ from which terrorists apparently originated. Police forces and other state agents should make sure to act evenhandedly in order to (re-)build a relationship of trust, thereby making any inclination to engage in ‘private policing’ unnecessary.

4. *Encouraging recruitment to the military and the police from every segment of society* to reduce the distance between state and society.

**Fight the Divisions**

Terrorism requires a framework to be correctly understood. Such a framework can be a narrative which, in the immediate aftermath of an attack, gives people a sense of understanding what is going on. Erving Goffman defines a “framework” as a “cognitive and practical structure for organizing social experience, enabling us to understand what is happening to us and to take part in it.” A framework is not just an interpretation, but it also frames operations and decides on the best way to react to them. Gérôme Truc has shown how 9/11 resulted in an ill-defined framework. Following the hijacking of the four planes, no one initially knew what was happening and whether this was an accident or a terrorist act. Several political statements and press releases then contributed to shedding light onto the nature of the events. Framing a post-attack narrative proves essential for delineating the nature of the event and helps to identify who is the adversary and how the threat should be dealt with. Such a framework also contributes to defining the borders of the in-group community, and, in doing so, points to the direction taken by phenomena such as revenge and vigilantism.

Revenge needs a clear enemy. Bjørgo and Mareš showed how specific groups (migrants, minorities) could become objects of fear and, sometimes, even hatred. In order to prevent revenge acts and vigilantism, those leading state and civil society should make efforts to reduce every form of societal divide which can generate (further) polarization. Social cohesion can help to avoid scapegoating phenomena and revenge acts. A cohesive society is unlikely to support the unauthorized use of violence against its members. Therefore, providing a framework that reduces internal divisions can help to achieve what Bjørgo and Mareš referred to as “Lack of support for vigilante groups and activities from the public, politicians or the news media.”

Measures from this category should be taken by government actors, but also – and more importantly – through religious and community leaders, local authorities, and international organizations, in a citizen-oriented fashion.

Prevention of revenge acts and vigilantism should include the following measures in order to minimize internal divisions that can feed community resentment and scapegoating, thereby feeding passions calling for revenge:

1. Establishing a *clear distinction between terrorists and ordinary citizens* sharing the same faith or political cause as those who engaged in terrorism. Making an entire minority or diaspora community responsible for the misdeeds of a few of its members can only lead to more marginalization and create a ‘suspect community’, thereby providing fertile grounds for individual revenge actions and collective vigilantism. Government actors, local authorities, community and religious leaders, civil society initiatives, media and even international organizations can play a role in making this distinction clear.
2. **Promoting inter-community dialogue**, through common activities, conferences, meetings. Centuries ago, the Arab philosopher Averroes had already recognized that “ignorance leads to fear, fear leads to hate, and hate leads to violence.” Reinforcing inter-community dialogue can increase understanding between the communities and show to all that there is a common interest in moderation and in rejecting extremism that leads to violence. Such measures should preferably emerge from the local, community level, in a bottom-up perspective. International organizations can also contribute to promoting such dialogue, especially through its human rights initiatives.

3. **Promoting neutral, inter-community media** that offer a balanced perspective of the conflict, without associating entire sub-categories of society with terrorists who claim to act in their name.

4. **Properly countering statements that seek to recall again and again past terrorist attacks** in order to stigmatize and marginalize entire communities.

### Fight the Means

Revenge acts and vigilante activities are mostly about using force without proper authority. Vigilantes seek access to arms, and training for using these. Some countries only have weak legislation regarding the possession of arms in private hands. In the US, the second amendment to the Constitution grants individuals the right to keep and bear arms which, historically, has greatly facilitated vigilantism. However, in other countries – e.g. in New Zealand after the Christchurch attacks – decisive steps have been taken, e.g. against the acquisition of assault weapons. Measures in this category fall onto those holding sovereign powers, namely the legislative and judiciary branches of the State. In general, measures to prevent revenge acts and vigilantism should include the following in order to make it harder for people to obtain tools for violence.

1. **Reviewing legislation on the private possession and use of arms.** The sale of arms to a broad section of the public with insufficient background checks tends to facilitate phenomena of private justice and punishments, feeding acts of revenge and violence.

2. **Ensuring accountability and judicial sanctions against those who act as vigilantes and avengers.** People who used force for private ‘justice’ outside a rule of law framework should be brought to justice. Judicial sanctions deter other wannabe vigilantes from applying their private notions of justice. Such sanctions promote and reinforce the rule of law and strengthen respect for the rule of law.

Prevention of private revenge acts and vigilantism in response to major terrorist acts and campaigns of terrorism should focus on alternative and constructive methods of public response. For example, after the 2011 Breivik attacks in Oslo and Utøya, the dignified public commemorations met the Norwegian people’s desires to “do something” after the killing of 77 people by a lone right-wing extremist. Ten years prior, in response to the 9/11 attacks, there were similar activities detectable. However, these responses were on a lesser scale and not spearheaded by the government. Gérôme Truc highlighted several peaceful 9/11 demonstrations:

“Organized at the behest of American pacifist associations, Protestant churches and left-wing organizations such as the online mobilization platform MoveOn, the placards read: ‘Break the cycle of violence’, ‘War is not the answer’, ‘It’s time for reflection, not revenge’ and ‘An eye for an eye leaves the whole world blind.’”

---

*ROBIN 1045*
Yet, this type of reaction has not become mainstream or government policy. Instead, the American government declared a ‘Global War on Terror’ and, as a result, almost twenty years later, jihadist terrorism is much stronger than before 9/11.

**Conclusion**

This chapter has identified four different types of responses that can emerge in the immediate aftermath of a major terrorist attack or in the wake of a campaign of violence. Some of these reactions, especially when they involve the unauthorized use of private violence, are dangerous for state and society, as well as for a successful counterterrorism campaign. Preventing private violent responses to terrorism will require governments to show their ability and willingness to act decisively, while staying within the confines of the rule of law. Both civil society and government actors should strive to reduce domestic polarization since that tends to feed the desire for vengeance and reprisals.

*Marie Robin is a PhD candidate affiliated with the Center for War Studies at the University of Southern Denmark, and the Centre Thucydide at Université Paris 2 Panthéon-Assas. Her dissertation proposes a conceptualization of the role of revenge in International Relations by analyzing the revenge narratives of the Islamic State, Al Qaeda, and Boko Haram. For her dissertation, Marie received funding from DGRIS/IRSEM. She presented her research at ISA Toronto, EISS Paris, as well as various national conferences. Marie taught courses of Ethics and of International Relations at Sciences Po, at the Université de Lille, and at the University of Southern Denmark. She also organized the first edition of the Graduate Conference of the War Studies Network in January 2020. In addition to her PhD, she works as a research assistant and translator for various academic publications and centers.*
Endnotes

1 Translation: ‘You won’t have my vengeance’. These words paraphrase the title of a book written by Antoine Leiris, who lost his wife in the Bataclan concert hall attack in Paris in November 2015. Titled Vous n’aurez pas ma haine (“You will not have my hatred”), his book advocated peace and asked state and society to prevent new cycles of violence at all cost, by refusing to give in to feelings of hatred and acts of revenge. See: Leiris, Antoine, Vous n’aurez pas ma haine, Paris: Fayard, 2016.

2 On the political impact of revenge, see: Christensen, Kit R., Revenge and Social Conflict, Cambridge: Cambridge University Press, 2016.


6 For instance, in 2015, the then French Minister of Defence, Jean-Yves Le Drian, wrote a book: Who is the enemy? trying to answer this crucial question so as to explain the foreign policy orientations that followed the 2015 attacks in Paris. See: Le Drian Jean-Yves, Qui est l’ennemi?, Paris: Les Editions du cerf, 2016.


8 Ibid., p. 5

9 ‘Mémorial de Caen’ is a museum based in Caen, Normandy, which focuses on the history of the Second World War and the D-Day Operation of 6 June 1944.

10 Truc, Gérôme 2016, p. 25.


15 Truc, Gérôme 2016, p. 32.

16 Ibid.
17 Merriam-Webster dictionary: “revenge.” Available at: https://www.merriam-webster.com/dictionary/revenge
19 Raymond Verdier defined vengeance as “Both a virtue when it defends a person’s dignity and a vice when it becomes a passion for destruction” (translated by MR), in: Verdier, Raymond Vengeance. Le face-à-face victime/agresseur, back cover.
22 The Christchurch Manifesto in the author’s (MR) archive.
31 Ibid.
Although the issue of target identification is essential to vigilante and revenge activities, its analysis remains highly context dependent. We acknowledge that political opinions, xenophobic sentiments, socialization, culture, emotions and even mistakes, can play a major role in the identification of targets. Specific case studies of vigilant and vengeful behaviors will be able to deal with the choices made in this respect. For our general purpose, we posit that the avengers’ preferences will follow the three-step process described below: avengers and vigilantes will preferably target the terrorist, then the terrorist group, then what they deem to be his/her community of belonging. On this issue, see for example: Rosenbaum H. Jon and Peter C. Sederberg, “Vigilantism: An Analysis of Establishment Violence”, Comparative Politics, 6:4, July 1974, pp. 541-570.


Tore Bjørgo and Miroslav Mareš distinguish four different types of vigilante activities, depending on their modus operandi, namely: (1) Vigilante terrorism/pogroms/lynchings; (2) paramilitary militia movements; (3) border patrols; (4) street patrols. In this typology, only type (1) overtly uses violence. Situations (2), (3) and (4) display force capacities but an actual use of these capacities is not automatic. Some scholars have identified case (1), i.e. vigilant terrorism as a subtype of terrorism. See: Bjørgo, Tore and Miroslav Mareš (eds.), Vigilantism against Migrants and Minorities. New York: Routledge, 2019; quoted from MS, p. 1; Sprinzak, Ehud, “Right-Wing Terrorism in a Comparative Perspective: The Case of Split Delegitimization”. Terrorism and Political Violence, Vol. 7, No 1, 1995.


Fourchard, Laurent 2018, p. 184.

Bjørgo and Mareš 2019.


On this issue, see, among others, Lee,Traci G., ‘The Real Story of Sunil Tripathi, the Boston Bomber Who Wasn’t”, NBC news, 22 June 2015. Available at:...


47 On this issue, see Zech 2015.


51 On Génération Identitaire, see the information box below.


58 On this case, see Anderson, Charles, Christchurch shooting suspect will face 50 murder charges, say New Zealand police”, *The Guardian*, 4 April 2019.

59 Christchurch manifesto, source: the author’s personal archives.

60 Thurston 2018.

61 The state of emergency was implemented in May 2013. The activities of the jihadist group Boko Haram, seeking to establish a sharia-based Islamic State around the Nigerian city of Maiduguri motivated this decision. BH had overtly declared being at war against the Nigerian state. President Goodluck Jonathan had declared a state of emergency so as to give a free hand to the Nigerian security forces for dealing with Boko Haram. The president has been widely criticized on the international stage for the military’s indiscriminate and extremely violent operations in the fight against BH. According to Human Rights Watch, the military had burned more than 2000 homes and killed 183 people in a raid on Baga, one month before the introduction of the state of emergency.

Thurston 2018, p. 207. Emphasis in italics by MR.


Silke 1999, p. 56.

Ibid.


This is also highlighted by Christensen, Kit R., *Revenge and Social Conflict*, Cambridge: Cambridge University Press, 2016.


On this issue, one can refer to Greek mythology with a particular focus on Medea’s revenge. In order to avenge herself for her husband Jason’s treason, Medea decided to kill her children, thereby hurting herself in order to achieve her vengeance. On a similar vein, Antigone’s revenge for her brother resulted in her being buried alive. Desperate to complete his/her revenge, some avengers do not fear harming themselves as well.

Interview with a French victim of terrorism, Paris, July 2019.

Ibid.


Thurston 2018, pp. 207-209.


Bjørgo, Tore and Miroslav Mareš 2015.

Fourchard 2018, p. 171.

Favarel Garrigues and Gayer 2015, p. 23.
87 Zech 2015.
94 Bjørgo and Mareš, 2015, pp. 9-11.
96 Ibid., p. 8.
98 Truc, Gérôme 2016, p. 15.
Bibliography


Web-based Resources


European Eye on Radicalization. Available at: https://eeralradicalization.com

International Center for Counter-Terrorism (ICCT), entry “Revenge”: https://icct.nl/?s=revenge.

Pôle de recherche sur l’analyse du vigilantisme (Research initiative on vigilantism, in French), CERI Sciences Po. Available at: https://www.sciencespo.fr/ceri/fr/content/pole-de-recherche-sur-lanalyse-du-vigilantisme.


SIPRI, Yearbook Online, entry ‘Vigilantism’ and ‘Revenge’. Available at: https://www.sipriyearbook-org.

Vox-Pol. Available at: https://www.voxpol.eu.

World Justice Project. Available at: https://worldjusticeproject.org
Chapter 34

Prevention of Human Rights Violations and Violations of International Humanitarian Law while Fighting Terrorism

Tom Parker¹

Terrorism is a contingent political strategy. At the outset, terrorist groups are by their very nature marginal, lacking in popular support, and limited in terms of the physical force they can project. Even the weakest states are powerful in comparison, blessed with far more substantial resources in terms of men, material and treasure. Left to their own devices, terrorists will rarely possess sufficient force to successfully attain their political goals. The genius of generations of terrorist planners has been to explicitly seek to turn the state’s strength to their advantage, provoking government after government to overreact to the threat they pose by introducing draconian security measures, curtailing civil liberties, and infringing established human rights protections. This in turn results in a greater polarization of the population, the radicalization of greater numbers of the terrorists’ potential constituents, and the undermining of the state’s legitimacy both at home and abroad. This strategy has been appositely described as “political jujitsu.” Furthermore, contemporary social science research into individual processes of radicalization suggests that witnessing or experiencing abuse at the hands of state officials is a leading driver of violent extremism. Adhering to international human rights law can help prevent states from falling into the terrorists’ trap, and making a bad situation commensurately worse.

Keywords: detention, human rights, overreaction, SITs, targeted killing, terrorism, torture.
“The ‘security forces’ set about their work in a manner which might have been deliberately designed to drive the population into our arms. On the pretext of searching they burst into people’s homes by day and night, made them stand for hours with their hands up, abused and insulted them.... Anyone who protested had scant hope of getting justice.”

- EOKA commander General Georgios Grivas

“Every fella who gets his head cracked open by a [policeman’s] baton is a potential recruit.”

- Provisional IRA Volunteer Des Long

The “war of the flea” metaphor popularized by Mao Tse-tung and Robert Taber to explain the asymmetrical challenge guerrilla warfare poses to government authority has endured because it works on several levels. A single flea, like a single terrorist, is itself relatively inconsequential, although acting in concert with other fleas it can become a serious irritant for the host. However, the real damage is done not by the flea’s bites but by the host’s response – the self-inflicted wounds caused by scratching at the bites, which may even become infected leading to serious illness. Terrorism operates on the same principle. It is a contingent political tactic. The uncomfortable reality is that the existential threat posed by terrorism is not posed by the attack itself - it is posed by how we respond. The temptation for states is to reach for the coercive tools in the tool box, to fight fire with fire, to turn, in former US Vice-President Dick Cheney’s memorable phrase, to the dark side. When states give into this temptation, which they invariably do, they are falling into the trap that has been set for them.

While a terrorist attack may have devastating implications at the individual level, in strategic terms a terrorist event – even one of the unprecedented magnitude of the September 11th attacks - rarely poses a meaningful challenge to the survival of the state. However, by reacting as if it does, States often overturn established norms of behavior, longstanding social compacts, and erode hard won civil liberties protections that shield their citizens from a far more ubiquitous set of social ills such as public corruption, miscarriages of justice, the abuse of power by government officials, and systemic discrimination. This can change a society far more dramatically than any terrorist attack. Terrorists understand this dynamic all too well and they calibrate their attacks to exacerbate this effect. Indeed, terrorist groups actively seek to put the coercive organs of the state to work on their behalf — as the terrorism researcher Louise Richardson has noted, “part of the genius of terrorism is that it elicits a reaction that furthers the interests of the terrorists more often than their victims.”

There is nothing particularly new about Louise Richardson’s insight – governments have simply chosen to ignore it. As early as 1975, the writer and historian David Fromkin published an important, but sadly now neglected article, in Foreign Affairs entitled The Strategy of Terrorism in which he argued that “terrorism is the indirect strategy that wins or loses only in terms of how you respond to it.” Even though Fromkin was writing primarily about the Marxist terrorist groups that plagued Western Europe in the 1970s, like the German Rote Armee Fraktion (Red Army Faction) and Italian Brigate Rosse (Red Brigade) as well as earlier anti-colonial movements such as the Algerian Front de Libération Nationale (National Liberation Front, or FLN) and Zionist group Irgun, his analysis remains as relevant today as the day he penned it. Critically, he understood that “terrorism wins only if you respond to it in the way that the terrorists want you to; which means that its fate is in your hands and not in theirs. If you chose not to respond at all, or else to respond in a way different from that which they
desire, they will fail to achieve their objectives.” He also warned that “brutality is an induced governmental response that can boomerang. It is this ability to use the strength of repression against itself, in many different ways, that has enabled terrorist strategies to succeed.” Fromkin christened this strategy “political ju-jitsu.”

Political ju-jitsu is a martial art that terrorist groups have long understood. In A General Theory of Power Control, the influential military strategist Rear-Admial Joseph C. Wylie wrote that “the primary aim of the strategist in the conduct of war is some selected degree of control of the enemy for the strategist’s own purpose.” By crafting attacks designed to provoke a draconian state response, this is precisely what terrorists aim to do, and, by exploiting the inevitable societal polarization that results, they hope to attract new recruits to their banner while undermining the state’s own claim to be acting legitimately. This specific intent can be found clearly expressed in numerous internal terrorist group documents, memoirs, political communiqués and manifestos. In fact, there is more than enough evidence to suggest that this strategic approach amounts to what might legitimately be described as terrorist doctrine. The fields of sociology, anthropology, and political science have all generated similar theories about the contagiousness of ideas to explain the diffusion of innovative practices across societies. Peter Waldmann, Martha Crenshaw and Mia Bloom have all applied this concept to suggest variously that a “contagion” or “demonstration” effect acts to spread ideas from terrorist group to another, arguing that the perceived success of some groups attracted others to emulate aspects of their approach. Intuitively anticipating this effect, early modern terrorists expressed the hope that they would set an example for others to follow, with the Russian populist Nikolai Morozov observing that “when a handful of people appears to represent the struggle of a whole nation and is triumphant over millions of enemies, then the idea of terroristic struggle will not die once it is clarified for the people and proven it can be practical.” In July 1881 the anarchist congress in London passed a formal resolution agreeing “it is absolutely necessary to exert every effort towards propagating, by deeds, the revolutionary idea and to arouse the spirit of revolt in those sections of the popular masses who still harbor illusions about the effectiveness of legal methods.”

Even the most cursory inspection of the historical record confirms the suggestion that terrorists learn from the experiences of their peers, that they read material generated by other militant groups, even across ideological divides, and that they are enthusiastic consumers of the tactical and strategic primers produced by their predecessors. For instance, the Indian nationalist Barin Ghose, jailed for his role in a 1909 conspiracy to assassinate a member of the British government administration in Bengal, wrote that his “cult of violence” was “learnt from the Irish Sinnfeinners [sic] and Russian secret societies.” The Egyptian theocrat Sayyid Qutb urged his fellow Islamists to learn from the success that the Jewish terrorist groups Lohamei Herut Israel (Fighters for the Freedom of Israel, or LEHI) and Irgun Zvai Leumi (National Military Organization, or Irgun) had enjoyed influencing the British policy in Palestine. LEHI’s Avigad Landau in turn studied the operational practices of the Irish nationalist movement, Narodnaya Volya (People’s Will) and the Serbian Black Hand, and Avraham Stern, out of whose eponymous militant group LEHI evolved, translated excerpts of P.S. O’Hegarty’s book The Victory of Sinn Féin into Hebrew. The FLN bomber Zohra Drif recorded in her memoirs: “We read a lot and were very influenced by the writings of the Bolshevik Revolution, the Spanish Civil War, and the anti-Nazi resistance.” Yasir Arafat’s intelligence chief Salah Khalaf, better known to posterity by his nom de guerre Abu Iyad, noted in his memoirs: “The guerrilla war in Algeria, launched five years before the creation of Fatah, had a profound influence on us.” Dimitris Koufodinas, Operations Chief of the Greek terror group November 17, taught himself Spanish in his prison cell so he could translate the prison memoirs of two Tupamaros leaders, Mauricio Rosencof and Eleuterio Fernández Huidobro. Provisional IRA commander Brendan Hughes reported reading speeches by Che Guevara and Fidel Castro in prison, while Provisional Sinn Féin President Ruairí Ó Brádaigh distributed seven copies of Robert Taber’s
classic study of guerrilla warfare, *The War of the Flea*, to each member of the Provisional IRA’s Army Council. 

The current leader of al-Qaeda, Ayman al-Zawahiri, published a critique of the “shortcomings” of the Society of the Muslim Brothers in 1991 entitled *The Bitter Harvest*, and the Norwegian white supremacist Anders Behring Breivik quoted extensively from the Unabomber, Theodore Kaczynski, in his own political manifesto, telling his court-appointed psychiatrists that he had learned much from studying al-Qaeda.

The idea that the state could be deliberately provoked into acting in such a manner that would serve to give rise to further opposition was born on the revolutionary left. In a series of articles written between January and October 1850 for the *Neue Rheinische Zeitung’s Politisch-ökonomische Revue* (and republished by Friedrich Engels in 1895 under the title *The Class Struggles in France 1848–1850*), Karl Marx reflected on the lessons revolutionaries could learn from the failure of the widespread uprisings that occurred across Europe in 1848, concluding that the socialist cause “made headway not by its immediate tragi-comic achievements, but on the contrary by the creation of a powerful, united counter-revolution, by the creation of an opponent, by fighting which the party of revolt first ripened into a real revolutionary party.”

Pierre-Joseph Proudhon’s influential *General Idea of the Revolution in the Nineteenth Century* published a year later in 1851 was even more explicit, in an opening section entitled *Reaction causes Revolution* the French anarchist philosopher wrote:

> “a revolution cannot be crushed, cannot be deceived, cannot be perverted, all the more, cannot be conquered. The more you repress it, the more you increase its rebound and render its action irresistible… Like the Nemesis of the ancients, whom neither prayers nor threats could move, the revolution advances, with somber and fatal step, over the flowers cast by its friends, through the blood of its defenders, across the bodies of its enemies.”

One of the first apostles of terrorist violence to avowedly adopt this strategy was the Russian anarchist Sergei Nechaev whose *Catechism of the Revolutionist* advises readers that violent officials should be “granted temporary respite to live, solely in order that their bestial behavior shall drive the people to inevitable revolt.”

Nechaev also notes in his *Catechism* that once the government in power begins to realize the inevitability of a popular revolt it will use “all its resources and energy toward increasing and intensifying the evils and miseries of the people until, at last, their patience is exhausted and they are driven to a general uprising.” Nechaev developed a theory of political provocation in which he aimed to push young radicals into direct confrontation with the authorities resulting in “the traceless death of the majority and a real revolutionary formation of the few.”

As he told one public meeting in Russia:

> “I have only one, though strong, hope in the government … Let it imprison more students, let students be expelled from universities forever, let them be sent to Siberia, thrown out of their tracks, be stunned by the persecution, brutality, unfairness and stupidity. Only then will they harden in their hatred to the foul government, to the society which heartlessly watches all the atrocities of the government.”

Nechaev’s theme was picked up by other anarchist militants including the anarchist prince Peter Kropotkin who wrote in another influential text, *The Spirit of Revolt*:

> “The government resists; it is savage in its repressions. But, though formerly persecution killed the energy of the oppressed, now, in periods of excitement it produces the opposite result. It provokes new acts of revolt, individual and collective, it drives the rebels to heroism; and in rapid succession these acts
spread, become general, develop. The revolutionary party is strengthened by elements which up to this time were hostile or indifferent to it.”

In the aftermath of the Easter Uprising in 1916 the British General Sir John Maxwell was dispatched to Ireland to impose order and he took the view that it was “imperative to inflict the most severe sentences” on the organizers of the uprising and the commanders who took part “to act as a deterrent to intriguers and to bring home to them that the murder of His Majesty’s subjects or other acts calculated to imperil the safety of the realm will not be tolerated.”

Fourteen ringleaders of the uprising were sentenced to death in Dublin, and also two other conspirators, Thomas Kent and Roger Casement, in Cork and London, respectively. But all that General Maxwell actually managed to achieve, in the words of one of the pioneers of urban guerrilla warfare, Michael Collins, was to awake “the sleeping spirit of Ireland.”

When Irish nationalists launched new attacks against the British authorities in 1919 the British again turned to coercive measures to try to put down the revolt, including the creation of a Special Reserve of temporary constables recruited from the ranks of World War I veterans who became known as the Black and Tans and were associated with some of the worst excesses of British rule, and again these measures backfired. The IRA had learned from Easter Uprising and were quick to exploit British brutality to grow their ranks. An incident in December 1920 illustrated the IRA’s strategy in operation. A company of Royal Irish Constabulary Auxiliaries responded to an IRA ambush that killed one officer and wounded eleven others by sacking the center of Cork in an orgy of looting and violence. An IRA man who witnessed the destruction told the reporter James Gleeson: “We could have shot most of them that night if we had wanted to… but it would have ruined the whole show. They were doing all they could to help us.”

The IRA gunman Dan Breen would later note in his memoirs: “The frightfulness of the Tans proved a boomerang against those who had cast it, for the people were finally goaded into such fury that they made up their minds, ‘come hell or high water’, never to give way before such tyranny.” The IRA would go on to formally integrate the lessons of the 1919–1921 Anglo-Irish War into its operational doctrine. The Handbook for Volunteers of the Irish Republican Army issued during the 1956–1962 cross-border campaign established three main strategic goals for the nationalist movement:

“(1) Drain the enemy’s manpower and resources; (2) Lead the resistance of the people to enemy occupation; (3) Break down the enemy’s administration … [The volunteer] achieves the second by remembering that the people will bear the brunt of the enemy’s reprisal tactics and inspiring them with the aims of the movement.”

In British Mandatory Palestine, Zionist militants adopted a similar concept of operations to the IRA, whose successful independence struggle they had closely studied. David Fromkin recalled attending a meeting in New York City in 1945 as a youth where he heard “one of the founders of the Irgun” explain how the organization expected to defeat the British:

“To do so… his organization would attack property interests… This, he said, would lead the British to overreact by garrisoning the country with an immense army drawn from stations in other parts of the world. But postwar Britain could not afford financially to maintain so great an army either there or anywhere else for an extended period of time. Britain urgently needed to demobilize its armed forces. The strain would tell; and eventually economic pressure would drive the Attlee-Bevin government either to withdraw from Palestine or else to try some reckless and possibly losing gamble in an effort to retrieve the situation.”
The leaders of Irgun also understood the propaganda value of highlighting any abuses committed by the British security forces and were not shy exploiting British missteps to draw unflattering comparisons between British rule and Nazi Germany on the international stage. The Head of Irgun, and subsequent Prime Minister of Israel, Menachem Begin, later wrote: “We knew that Eretz Israel, in consequence of the revolt, resembled a glass house. The world was looking into it with ever-increasing interest and could see most of what was happening inside.” The cumulative effect of this strategy was not lost on the British themselves. The Joint Planning Staff of the British War Office concluded in a March 1947 assessment of security options for confronting Zionist terrorism in the British Mandate of Palestine that both Irgun and LEHI “wish to force us to employ sterner measures which can be represented as punitive against [the] community, thereby swinging moderate opinion against us and obtaining more recruits for themselves.” Yet, despite some apparent awareness of the trap they faced, the increasing tempo of attacks nevertheless still propelled the British headlong into it.

Georgios Grivas, the commander of EOKA (The National Union of Cypriot Combatants), the Greek-Cypriot movement that campaigned for union with Greece during the 1950s, was also quick to understand how the strength of the British forces could be turned to his advantage as he sought to bring British colonial rule on the island to an end:

“[T]here went on a continuous struggle as to which of the two opponents would win the population over to his side. The weapon used by the British was force. But it was found that the harsher the measures resorted to by the British, the more the population became estranged from them and inclined to our side… The representatives of Britain in Cyprus, both soldiers and civilians, behaved towards the inhabitants with an animosity which was far from politic.”

In his primer on guerrilla tactics, Guerrilla Warfare and EOKA’s Struggle, Grivas stressed the importance of mobilizing the youth — as “a testing ground and nursery from which I selected fighters for my groups of guerrillas and saboteurs” — describing in detail the effect of the so-called “Battle of the Flags” waged by Greek Cypriot schoolboys against the British authorities. When the British banned any public display of the Greek national flag, Grivas issued an order designed to bring schoolchildren into the struggle for union: “See that the Greek flag is flown from all elementary schools and is kept flying.” The British responded by closing schools, detaining those responsible, and sometimes their teachers, as well as by doling out beatings on the spot. Grivas scornfully recalled, “this stupid and ill-advised action on the part of the British was exploited by me for the purpose of exciting still further the fanaticism of the young pupils,” and he described how this fanaticism enabled him to use schoolboy recruits between the ages of fourteen and seventeen to undertake dangerous missions “such as blowing up aircraft at the British airbases, the laying of mines and blowing up of police stations.”

During the Algerian war of independence, the FLN’s leading military strategist, Ramdane Abane, promoted an approach designed to provoke the French authorities to “accelerate repression” arguing that harsh French counter-terrorism measures would force the Algerian population to turn to the FLN for protection. Abane believed that only the way to separate the Algerian population from the French colonial system, with all its cultural baggage, was to precipitate, in Martha Crenshaw’s words, a “sharp and brutal break.” Ramdane understood that attacks on civilian targets were the quickest way to achieve his goal and coined the cynical and much repeated aphorism, “one corpse in a jacket is always worth more than twenty in uniform.” The historian Alastair Horne has described the “Philippeville massacre” of 20 August 1955 as a textbook example of a terrorist group deliberately setting out to provoke an overreaction from the authorities. This was especially true of the murders that took place in the small pyrite mining settlement of El-Halia where thirty-seven French nationals, including
ten children, were butchered by FLN cadres in bestial fashion. El-Halia had enjoyed a reputation for excellent relations between the local French and Muslim residents and was deliberately targeted for this reason — to create a climate of distrust between the two communities. The viciousness of the killings, with bodies dismembered and desecrated, was intended to provoke a furious response from the French authorities and further polarize the population. The French response did not disappoint and the FLN later claimed almost 12,000 local Arabs had been killed in reprisal. 43 This in turn had the anticipated effect of boosting the FLN’s recruitment efforts - by October 1955, the FLN’s strength in the North Constantine region where the atrocities had occurred had increased from 500 to 1,400 regular volunteers. 44

Zohra Drif recalled being told by another key leadership figure in the FLN, Larbi Ben M’hidi, of the group’s intention to forcibly expose the true nature of French colonial rule and the oppression suffered by the native population of Algeria to the international community:

“Never lose sight of what we are - political activists whom the colonial regime’s arrogance has forced to become fighters in a war of national liberation… “[W]e will oblige France to meet us on a different battlefield - the political one, where it can never win. That is why our ambushes, our attacks, our bombs, and all the rest must help us to defeat France politically and to diminish it morally and symbolically... That is why each of our attacks. Each of our ambushes, each of our lives sacrificed must serve to unmask France before the world, to show that our people are at war against a foreign power occupying us by force... That is the meaning of the primacy of the political over the military, which is a fundamental principle of our revolution.” 45

As the French writer and philosopher Raymond Aron succinctly observed: “Even though the FLN had written the script, the French, with suicidal logic, went ahead to play the role for which they had been cast.” 46

Another key theorist of provocation was the Basque nationalist Federico Krutwig. In 1963, Krutwig published Vasconia, a treatise on Basque nationhood that would become a key text for the Basque separatist group ETA, despite the fact that Krutwig himself was not a member of the movement. José Luís Álvarez Enparantza, one of the original founders of ETA who was better known by his pseudonym Txillardegi, called Vasconia, “the most important book on Euskadi [the Basque homeland] published in this century” and it was endorsed by ETA’s Second Assembly. 47 Krutwig placed great emphasis on popular action and outlined in Vasconia what he termed his “Action–Repression–Action” theory of violence. In stage one, “the guerrillas” carry out a provocative violent action against the state; in stage two, the state responds in a heavy-handed fashion with repression against “the masses”; and in stage three, “the masses” respond in turn with a mixture of panic and rebellion, at which point “the guerrillas” carry out a new attack to begin the cycle again and push “the masses” into further acts of insurrection. 48 José Luis Zalbide synthesized the passages on armed struggle in Vasconia, along with liberal contributions from Mao and Guevara, into an operational manual entitled Insurrección en Euskadi (Insurrection in Euskadi) that was also formally adopted by ETA. Hardliners within ETA began to argue in favor of attacking senior regime figures in the hope of provoking Franco’s government into “excessive and non-discriminatory retaliation against all Basque residents,” and in 1964, ETA celebrated the success of this approach, crowing:

“We have achieved one of our major objectives — to oblige the enemy to commit a thousand wrongs and atrocities. Most of his victims are innocent. Meanwhile, the people, more or less passive until now, become indignant
against the colonial tyrant and, in reaction, come over entirely to our side. We could not have hoped for a better result.”

A former ETA activist elaborated further to the researcher Fernando Reinares:

“If killing a Civil Guard or twenty Civil Guards every other week is to serve any purpose of all… it was to bring about the Ulsterization of Euskadi, which was the theory that the milis [militants] were spouting around that time. The Ulsterization of Euskadi would mean [the Spanish government] putting soldiers on every street corner and then the people would witness the contradictions of power and see the true face of the oppressor and all that.”

The Marxist terrorist groups that rose to prominence in Latin America and Western Europe in the 1960s and 1970s were guided in large part by the writings of three theorists of guerrilla warfare: Mao Tse-tung, Ernesto ‘Che’ Guevara, and Carlos Marighella. Mao and Che were both somewhat skeptical about the strategic utility of terrorism— for Mao it was a transitory phase of People’s War intended to grow the revolutionary movement, and Guevara was initially concerned that was likely to provoke police oppression making the task of organizing the masses and other clandestine activity more difficult. While Mao remained true to his original vision, over time Guevara began to revise his opinion. Of the three, it was the Brazilian communist Marighella who most enthusiastically embraced terrorism as a strategic tool, and his *Mini-Manual of the Urban Guerrilla* would become a bible of sorts to a generation of Marxist-inspired terrorists from Montevideo to Berlin.

In his analysis of the potential weaknesses of the Japanese army occupying Chinese territory in *On Guerrilla Warfare*, Mao Tse-tung identified Japan’s “cruelty to the inhabitants of conquered areas” as a major area of vulnerability. Mao noted that because the Japanese soldier was both “a foreigner and a barbarian” Chinese guerrillas could “gain the confidence of millions of their countrymen.” He urged guerrilla commanders to intensify this effect by conducting “intensive guerrilla warfare” in areas controlled by the Japanese so that “in order to subdue the occupied territory, the enemy will have to become increasingly severe and oppressive,” ensuring that the gulf between occupied and occupier widened still further. Mao understood both the strategic importance of winning and maintaining public support, and also how easily security force personnel could be provoked into abusing the local population and so undermining their own position: “It is only undisciplined troops who make the people their enemies and who, like the fish out of its native element, cannot live.”

Following his successful experience with the Cuban Revolution in the Sierra Maestra, Guevara was unsurprisingly an enthusiastic proponent of the rural *foco* approach to insurgency also championed by his sometime comrade-in-arms, the French philosopher and activist Régis Debray. However, in his 1963 essay *Guerrilla Warfare: A Method* Guevara did acknowledge that urban fighters could also “perform actions of the greatest importance” and stressed the need to push the state to break its own rules:

“[W]e are passing through a stage in which pressure from the masses is very strong and is straining bourgeois legality so that its own authors must violate it in order to halt the impetus of the masses. Barefaced violation of all legislation or of laws specifically instituted to sanction ruling class deeds only increases the pressure from the people's forces… The people no longer support the old, and much less the new, coercive measures established by the dictatorship and try to smash them.”
His hope was that by stripping the “mask of democracy” from the state he could expose the true nature of the underlying oligarchy which he believed actually exercised power. By 1967 his views had hardened still further and he seemed to embrace the need for terrorist action, urging militants to “carry the war into every corner the enemy happens to carry it: to his home, to his centers of entertainment; a total war.” In Message to the Tricontinental Guevara wrote:

“It is necessary to prevent [the enemy] from having a moment of peace, a quiet moment outside his barracks or even inside; we must attack him wherever he may be; make him feel like a cornered beast wherever he may move. Then his moral fiber shall begin to decline. He will even become more beastly, but we shall notice how the signs of decadence begin to appear.”

Che believed the repression that resulted would not only provoke greater resistance to authoritarian rule, but would also harden rebels’ resolve by giving birth to “a relentless hatred of the enemy, compelling us over and beyond the natural limitations that man is heir to and transforming him into an effective, violent, selective and cold killing machine.”

Marighella was the only one of the troika to focus on operations conducted in an urban environment, arguing that in the face of urban terrorism “the government has no alternative except to intensify its repression … The people refuse to collaborate with the government, and the general sentiment is that this government is unjust [and] incapable of solving problems.”

Marighella theorized that a repressive state response would alienate the government from its population generating support for the terrorists, and that declining governmental legitimacy would strengthen the terrorist cause, as “the political situation in the country is transformed into a military situation in which the [government] appear more and more to be the ones responsible for the violence, while the lives of the people grow worse.” Practicing precisely what he preached, the Brazilian leftist group Ação Libertadora Nacional, established by Marighella in 1967, actually went so far as to spell out its intention to create a crisis that would provoke a military response in its founding manifesto. Marighella also demonstrated a particularly sophisticated understanding of public relations, writing that urban guerrillas should exploit by every possible means “the mistakes and the failures of the government and its representatives, forcing them into demoralizing explanations and justifications.”

Like Begin and M’hidi, Marighella appreciated the significance of the international dimension, and suggested making use of civil society organizations to put pressure on authoritarian rulers by “presenting denunciations to foreign embassies, the United Nations, the papal nunciature [sic], and the international judicial commissions defending human rights or freedom of the press, exposing each concrete violation and use of violence by the military dictatorship.”

In Uruguay, the National Liberation Movement - Tupamaros (MLN-T, more generally known as Tupamaros) set out deliberately to provoke a repressive response from the state and thus achieve the “transformation of a political situation into a military one.” They succeeded in achieving this goal, but subsequent events did not then turn out in their favor — in 1973, the Uruguayan military deposed the democratically elected civilian government and established a military junta that remained in power until 1985. Where the Tupamaros led others followed. Giangiacomo Feltrinelli, one of the founders of the Gruppi di Azione Partigiani (Patriotic Action Groups, or GAP), a precursor of Italy’s Brigitte Rosse, circulated a paper entitled Italy 1968: Political Guerrilla Warfare in which he urged leftist militants to “violate the law openly … [by] challenging and outraging institutions and public order in every way.”

He added: “When the state intervenes as a result, with police and the courts, it will be easy to denounce its harshness and repressive dictatorial tendencies.” Renato Curcio, one of the early leaders of the Brigitte Rosse, later echoed Feltrinelli’s insight in a public communiqué, explaining: “Faced with working-class terror, the bourgeoisie by now has an obligatory course — to reestablish control by intensified repression and progressive militarization of the state.”
Italian left labeled this concept of advancing revolutionary change “tanto peggio, tanto meglio,” literally “the worse, the better.”68 Amir Parviz Puyan, a prominent member of the Fadaiyan-e-Khalq (The Organization of Iranian People's Fedai Guerrillas), a Marxist–Leninist guerrilla group established in Iran in 1971, advanced much the same argument:

“By extending the violence against the resistance fighters, creating an unanticipated reaction, the repression inevitably hits all other oppressed milieus and classes in an even more massive way. As a result, the ruling class augments the contradictions between the oppressed classes and itself and creates a climate which leads of necessity to a great leap forward in the consciousness of the masses.”69

In a Rote Armee Fraktion pamphlet entitled Serve the People: The Urban Guerrilla and Class Struggle, that first appeared in April 1972, the authors outlined the group’s commitment to the Marxist concept of the dialectic of revolution and counterrevolution, quoting the North Korean communist leader Kim II Sung:

“It isn’t a question of whether we want the reactionary militarization or not; it is a question of whether we have the conditions necessary to transform the fascist militarization into a revolutionary mobilization, whether we can transform the reactionary militarization into a revolutionary one.”70

The pamphlet argued that the Federal Republic of Germany’s reaction to the RAF’s activities was playing straight into the group’s hands as those in power

“are obliged to violate their own system, and in so doing they show their true colors as enemies of the people — and the left creates accurate propaganda at a high dialectical level, as ought to be the case, when they say: ‘this terror is not directed against the RAF, but rather against the working class.’”71

Ulrike Meinhof returned to the same theme in a statement she made at her trial in September 1974 alongside Hans-Jürgen Bäcker and Horst Mahler:

“The enemy unmasks itself by its defensive maneuvers, by the system’s reaction, by the counterrevolutionary escalation, by the transformation of the political state of emergency into a military state of emergency. This is how it shows its true face — and by its terrorism it provokes the masses to rise up against it, reinforcing the contradictions and making revolution inevitable.”72

The idea that West Germany had never truly broken with its national-socialist past, and, that by engaging the security apparatus of the state, the RAF would force this hidden reality into public view, was one of the central operational principles underpinning the organization’s almost three-decade long campaign.73

Deeply influenced by Maoist People’s Wartheory — Palestinian cadres even received military training in China74 — Yasin Arafat’s Fateh evolved an explicit concept of operations that came to be known as al-taffir al-mutasalisil or “consecutive detonation.”75 Khalid-Hasan, who had been with Fateh more or less since its foundation, explained the logic of this strategy: “Our military action provokes an Israeli action against our people, who then become involved and are supported by the Arab masses. This extends the circle of conflict and compels the Arab governments either to join us or stand against us.”76 As one early Fateh publication, entitled A Statement on Timing, noted: “Any act of liberation that does not take conscious entanglement of the masses into
account will fail at the outset because it has over-looked the strongest active force in the battle.” The Popular Front for the Liberation of Palestine (PFLP) took a similar view — when the Israeli air force raided Beirut International Airport in December 1968 destroying thirteen Middle East Airlines passenger jets in reprisal for the attack on El Al Flight 253 in Athens two days earlier, the PFLP “thanked the Israelis for enlisting Lebanese support for the revolution,” concluding they “had helped the cause more than we dared contemplate by their prompt and decisive ‘reprisal.’” Harsh Israeli counter-terrorism measures also served to bolster the “narratives of brutality and injustice” that psychologically enable individuals to embrace violent opposition and endure the privations of clandestine warfare. Many Israeli security officials have come to appreciate the dilemma they face — Ami Ayalon, who served as the Head of the Israeli security service Shin Bet in the late 1990s, has implicitly acknowledged the effectiveness of consecutive detonation as a strategy: “War against terrorism is part of a vicious cycle. The fight itself creates … even more frustration and despair, more terrorism and increased violence.”

When the Provisional IRA split from the Official IRA in December 1969, its newly constituted Army Council, led by Seán MacStiofáin, adopted a plan of action built around a three-stage approach to ending British rule in Northern Ireland: first, the defense of Catholic communities; second, a combination of defense and retaliation against the loyalist community and the British authorities; and third, a sustained offensive engagement with the British in a guerrilla campaign. The initial problem facing PIRA commanders was that the British Army had been deployed to Northern Ireland in August 1969 by the Labour government of Prime Minister Harold Wilson to restore order, after a summer of rioting and sectarian violence in which the local police force, the Royal Ulster Constabulary (RUC), had abandoned any pretense of impartiality and had sided wholeheartedly with the loyalist community. As such, even Joe Cahill, the Officer Commanding the PIRA’s Belfast Brigade and a member of the ruling Army Council, admitted, that when the British Army first deployed to Northern Ireland, “people were glad to see them because the [Official] IRA had betrayed them [by failing to protect Catholic neighborhoods].” The researchers J. Bowyer-Bell, M. L. R Smith and Rod Thornton all note that the Provisional IRA began a strategy of deliberate provocation of the British Army in early 1970. Gerry Adams’ biographer Colm Keena noted that as PIRA commander in Ballymurphy Adams’ tactics was “to prod the British Army into acting as an army.” Rod Thornton reported “another ploy designed to poison minds against the Army… was the supplying of bogus intelligence to soldiers about certain – innocent – individuals. These would then be wrongly arrested raising levels of local antipathy.” Tommy Gorman, a member of PIRA’s 1st Battalion in Andersonstown, explained the rationale:

“We were creating this idea that the British state is not your friend … and at every twist in the road they were compounding what we were saying, they were doing what we were saying, fulfilling all the propaganda … The British Army, the British government, were our best recruiting agents.”

From July 1970 onwards, the battle lines were drawn and the British Army increasingly began to employ the same tactics it had used in counter-insurgency operations overseas. In the face of escalating violence, and the first British military casualties, the government introduced internment — open-ended detention without charge for suspected terrorists — in August 1971, which only served to further alienate the Catholic population, as did the news that some of the internees had been subjected to coercive interrogation techniques including hooding, wall-standing, the use of “white noise,” withholding food and water, and sleep deprivation. This alienation was made complete on 30 January 1972 when British paratroopers fired on an anti-internment protest in Londonderry ultimately killing fourteen demonstrators and wounding twenty-eight, an event immortalized in the public consciousness as Bloody Sunday. The Provisional IRA’s tactic had
worked like a charm and Gerry Adams, who commanded PIRA’s 2nd Battalion in Belfast during this period, would later acknowledge that the attitude and presence of British troops had resulted in a “resurgence of national consciousness and an almost immediate politicization of the local populace.”99 The operational manual first distributed to volunteers by the Provisional leadership in 1977, known colloquially as the Green Book, drew a similar lesson: “We exploit the enemy’s mistakes by propagating facts. So it was with their murderous mistakes of the Falls Road curfew, Bloody Sunday and internment.”90

Shaoul Mishal, Avraham Sela and Andrea Nüsse have similarly argued that part of the motivation for Hamas in mounting attacks against Israeli targets during the First Intifada was to provoke a repressive response, thus further radicalizing the Palestinian population and boosting international support for the Palestinian cause.91 Beverley Milton-Edwards and Stephen Farrell have also described how Hamas exploits Israeli reprisals carried out in response to its operations — such as home demolitions — to stoke community anger and build its base.92 In August 2014, the Israeli Defense Forces published excerpts from a Hamas manual on urban warfare reportedly recovered during an offensive conducted against the Shuja’iya Brigade of the Al-Qassam Brigades. While the authenticity of the manual has been questioned in some quarters, it does seem to tally closely with the reported behavior of Hamas units on the ground in Gaza. A section of the manual notes that the destruction of civilian homes “increases the hatred of the citizens towards the attackers [the IDF] and increases their gathering [support] around the city defenders (resistance forces).”93 Hamas’ well-documented use of locations typically protected from being targeted under the laws of armed conflict, such as schools and hospitals, would also seem to fit this strategy — hostile fire originating from such a location can void its protection under international law, but the public relations fallout from shelling or bombing a school or hospital typically overshadows the potential legitimacy of a decision to retaliate against an enemy firing position.94

But perhaps the most successful example of a terror group deliberately setting out to provoke a counterproductive state response is also one of the most recent. The US journalist Alan Cullison scored a major scoop when he purchased two abandoned al-Qaeda computers from a “semiliterate jewelry salesman” who had looted them from al-Qaeda’s central office in Kabul. Reviewing the contents, Cullison came across internal communications discussing the likely outcome of the 9/11 attacks which made it clear that the strike was intended to have a unifying effect on the many disparate mujahidin factions and that, recalling the war in Afghanistan against the Soviet invaders, al-Qaeda leaders hoped 9/11 would have a galvanizing effect on the Arab world.95 In this respect at least, the attacks were profoundly successful. In a broadcast in November 2004, Osama bin Laden gleefully compared President George Bush to the cantankerous goat who according to an ancient parable willfully dug up a lost knife buried in the ground that was later used to slaughter it.96 Ayman al-Zawahiri had also long believed that drawing America’s Muslim allies into a wider conflict would be an effective strategy for mobilizing domestic resistance to their rule, writing in Knights under the Prophet’s Banner:

“We win … by exposing the regime to the Muslim people when it attacks us in defense of its masters, the Americans and the Jews, showing thereby the ugly face, the face of the policeman, the faithful hireling in the service of the occupier, the enemies of the Muslim umma (the community of the [Muslim] faithful).”97

In 2005, the al-Qaeda insider Abu Bakr Naji published The Administration of Savagery, serialized in seven installments in the online Sawt al-Jihad (Voice of Jihad)98 magazine, to explain al-Qaeda’s strategy in detail to its supporters around the world. Naji wrote that al-Qaeda set “a trap” for the United States in Afghanistan, which it then fell into — by seeking revenge
for the 9/11 attacks, Naji asserted, the United States had committed itself to operations that would inevitably intensify over time, provoking a backlash from the Muslim community.

Naji further argued that what had worked against the Soviet Union would work against the United States — indeed, he went on to suggest that it would actually be easier to defeat the “soft” United States because the Soviets had been much tougher opponents. Naji cited the Yale historian Paul Kennedy’s influential study *The Rise and Fall of the Great Powers* in support of his central thesis: “If America expands its employment of military power and extends strategically more than necessary, this will lead to its downfall.”

A copy of *The Rise and Fall of the Great Powers* was also found in bin Laden’s hideout in Abbottabad. Naji also noted that al-Qaeda would be able to attract more recruits as a consequence of being able to demonstrate America’s direct interference in the Islamic world. In much the same spirit, one al-Qaeda publication actually heralded the US invasion of Iraq with an article entitled *Thank You, Oh Zio-Crusaders.*

Quoting Osama bin Laden, the Islamic State in Iraq and the Levant (ISIL) articulated a similar strategy in an article entitled *The Extinction of the Grayzone,* published in the January/February 2015 issue of ISIL’s glossy English-language magazine *Dabiq:* “The world today is divided into two camps. Bush spoke the truth when he said, ‘either you are with us or you are with the terrorists.’ Meaning, either you are with the crusade or you are with Islam.”

To this end, ISIL has deliberately set out to “bring division to the world” and reduce the space for compromise, moderation and multicultural exchange — the “grayzone” of the article’s title — which it dismisses as the hideout of hypocrites. The article is explicit about ISIL’s intention to provoke through its actions a draconian crackdown on the Muslim communities living in Western countries: “Muslims in the Crusader countries will find themselves driven to abandon their homes for a place to live in the Khilāfah, as the Crusaders increase persecution against Muslims living in Western lands.”

The group’s ultimate objective is to manufacture a clash of civilizations in which no middle ground remains: “Eventually, the grayzone will become extinct and there will be no place for grayish calls and movements. There will only be the camp of imān versus the camp of kufr.”

Another ISIL publication, *Media Operative, You Are a Mujahid Too,* acknowledged that part of the intent behind its terrorist operations was to “infuriate” governments into precipitous policy responses that would only further alienate their Muslim populations, and echoing Ramdane Abane, ISIL leader al-Baghdadi told his followers in an August 2018 that one attack in the West was worth 1,000 in Iraq or Syria.

In December 2014, Ilich Ramírez Sánchez, better known as the notorious PFLP terrorist Carlos the Jackal who had been incarcerated in France since August 1994, sent the French academic and prominent terrorism expert, Gilles Kepel, a manuscript entitled *La guerre psychologique (The Psychology of War),* in which he cast an appreciative professional eye over the tactics adopted by al-Qaeda, ISIL and their affiliates:

“The jihadists have followed this line of psychological warfare with great success in the media. The decapitations now carried out openly by citizens of countries that are members of NATO, transmitted over the Internet, are a magisterial media coup with immense, unparalleled benefits... Now the imperialist states will be subjected to reprisal attacks within their borders against which they cannot defend themselves, leading to indiscriminate repression which will multiply the recruitment of volunteers for jihad.”

If the fact that terrorists have been explicitly open about their desire to provoke an aggressive state response to their actions is not in itself enough to give national security hawks pause, then the social science research into the drivers of violent extremism produced in the past two decades should be. Radicalization is admittedly an extremely complex phenomenon. As the
founder of the CIA’s Center for the Analysis of Personality and Political Behavior, psychologist Jerrold Post, concluded after a lifetime spent studying terrorist profiles:

“There are nearly as many variants of personality who become involved in terrorist pursuits as there are variants of personality … Yet, no matter how justified the cause, no matter how repressive the society, there are some who join and some who don’t. Not every son of a Basque joins ETA.”

However, while there is little prospect of a universal theory of radicalization emerging any time soon, there is general agreement among researchers that radicalization is a process variously impacted to a greater or lesser extent by a range of what are often termed push (personal) or pull (societal) factors. These factors can be grouped into five broad categories – the psychological process of self-actualization sometimes also called the quest for significance, the social networks an individual belongs to, empathy for the suffering of others, social exclusion and marginalization, and personal experience of state repression. It is this last factor that is most relevant for this article.

As outlined above, terrorist leaders have long intuitively understood that violence begets violence and that aggressive government action against their constituents can be a powerful recruitment tool. David Fromkin understood this too when he wrote, “terrorism generates its own momentum.” Martha Crenshaw has argued that terrorist campaigns often come to resemble “a modern form of feuding” as action provokes reaction drawing more and more protagonists into the struggle and amplifying the anti-government frame within which militant groups operate. Louise Richardson identified “revenge” as one of what she described as the “three Rs” of terrorism—the others being “renown” and “reaction” — and this seems a constant theme across the literature. Mia Bloom also identified a desire for “revenge” as one of four primary motivations that she repeatedly encountered in her case studies of women terrorists (along with redemption, relationships, and a thirst for respect). In his influential study of micromobilization processes in 1970s Northern Ireland, the sociologist Robert White found that personal experience of state violence appeared to be a major determinant of individual decisions to embrace political extremism. In a series of interviews with Provisional IRA volunteers, White found that their personal interaction with British troops was cited again and again as they explained their decision to take up arms. Furthermore, he noted that Provisional IRA violence increased significantly in months following incidents in which the security forces harmed civilians or carried out particularly emblematic acts of repression, such as the introduction of internment. The desire to avenge a personal loss or humiliation is a powerful leitmotif running through many terrorists’ stories, and the stated intent to retaliate directly in response to government action is a commonplace feature of terrorist claims of responsibility. The following are just a small selection of examples taken from across the temporal and geographic spread of terrorist activity.

Perhaps the most iconic revenge story in the terrorism literature is that of Udham Singh. Legend holds that Udham Singh was among the wounded in the Jallianwala garden in Amritsar, India, in April 1919 when British troops under command of Brigadier Reginald Dyer opened fire on a crowd of protestors killing at least 379, and possibly as many as 1,000. Dyer had been sent to disperse the crowd by the British Lieutenant-Governor of Punjab, Michael O’Dwyer. Although Singh himself claimed to be a survivor of the massacre historians have not been able to find any independent confirmation of this, but as his biographer Anita Anand has noted whether Singh was there or not, what is beyond question is that the massacre had a transformative effect on him. Singh embarked on a life of revolutionary activity aimed at overthrowing British colonial rule. He joined the Ghadar Party and became a close associate of the prominent socialist revolutionary Bhagat Singh. The colonial authorities jailed him for four years in the late 1920s for the illegal possession of firearms,
and he was harshly treated in prison, but this did not deter him. Finally, on 13 March 1940, Singh walked into a public meeting at Caxton Hall in London where O’Dwyer was speaking and shot him dead. He also wounded the Secretary of State for India, the Marquess of Zetland. Singh was hanged for his crime, but he died content: “For a full twenty-one years, I have been trying to wreak vengeance. I am happy that I have done the job.”

Udham Singh’s story is perhaps a little more epic than most, but his motivation is common enough and occurs again and again in personal histories of terrorist actors from the earliest anarchist revolutionaries to the modern era’s Islamist extremists. Gaetano Bresci was an Italian immigrant living in Patterson, New Jersey, earning a living as a weaver. He was active in local anarchist circles and helped found and support an anarchist newspaper called *La Questione Sociale* (The Social Question). In May 1898, Bresci’s sister was one of at least 118 protestors cut down by canon fire in Milan during a protest against high bread prices, an incident that became known in Italy as the Bava-Beccaris massacre after the general who had ordered his troops to fire on the protestors.119 King Umberto I had subsequently awarded General Fiorenzo Bava-Beccaris the Great Cross of the Order of Savoy in recognition of his “brave defense of the royal house” prompting Bresci to mark the King as the target of his revenge. Bresci raised the money for a ticket home and traveled to the Lombard city of Monza where, in July 1900, he shot the King four times with a revolver he had brought with him from the United States, killing him. The leading Italian anarchist Errico Malatesta had long worried that personal motivations were beginning to overwhelm the principled ideological commitment of his comrades, commenting sadly: “It’s no longer love for the human race that guides them, but the feeling of vendetta joined to the cult of an abstract idea.”120 The most famous anarchist bomber of the belle époque, Émile Henri, was similarly motivated by a strong desire for revenge, for his father’s exile to Spain after the defeat of the Paris Commune where he died in penury, for the harsh treatment of striking miners by the Carmaux mining company, and for the execution of Auguste Vaillant following his attack on the Chamber of Deputies of the French National Assembly. Henri explained to the court during his trial for the February 1894 Café Terminus bombing:

“The bomb in the Café Terminus is the answer to all your violations of freedom, to your arrests, to your searches, to your laws against the Press, to your mass transportations, to your guillotinings…You have hanged us in Chicago, decapitated us in Germany, garroted us in Xerez, shot us in Barcelona, guillotined us in Montbrison and Paris, but what you can never destroy is anarchy.”121

A member of the Zionist Stern Gang detained by the British Mandate authorities in Palestine, Yitzhak Reznitsky, offered a strikingly similar rationale to his interrogators to explain why the group had mounted a flurry of bomb attacks on the Palestine police in April–May 1942:

“The severe methods employed by the police… including the shooting of Zak, Amper, Sevorai [sic], Lевштейн [sic] and Stern himself… convinced the members of the group of the Government’s intention to crush their organization at any cost, and it was decided to fight back.”122

Another leading member of the Stern Gang, Nathan Yellin-Mor, later wrote: “The first goal for a revenge attack was perfectly clear—Geoffrey Morton, the murderer of Yair [Stern].”123 Morton narrowly escaped an IED explosion along his route to work, and other devices targeted the Inspector General and Deputy Inspector General of the Palestine Police. Likewise, the May 1947 murder of Alexander Rubowitz, a young Jewish Brit Hashmonaim activist, snatched off the streets by the British undercover unit led by Major Roy Farran, prompted LEHI to mount a
wave of reprisal attacks that included the shooting of four British soldiers on a Tel Aviv beach, themurder of a British officer in a restaurant in Haifa, and the mailing of a parcel bomb to Farran’s family home in Staffordshire, which detonated killing his brother Rex. An Irgun statement issued in August 1939 proclaimed: “A hitting fist must be answered with two hitting fists – a bomb explosion has to be replied with two bomb explosions.”

The French decision to execute two Front de Libération Nationale members, Ahmed Zabana and Abdelkader Ferradj, led to the outbreak of the Battle of Algiers on 19 June 1956. FLN commander Ramdane Abane ordered his subordinate in Algiers, Saadi Yacef, to “kill any European between the ages of eighteen and fifty-four. But no women, no children, no old people” and within seventy-two hours, forty-nine French civilians had been murdered in retaliation. Saadi Yacef later told the French intellectual Germaine Tillion: “It was the day when France decided to guillotine our fighters that the FLN and ALN decided to escalate the fight. Denying us dignity, even in death, is the ultimate provocation. We want to face death. We want to die standing up, not cut in two!”

White French settlers hit back with a series of bombings of Muslim neighbourhoods — including most notoriously the detonation on 10 August 1956 of a large explosive device in the Rue de Thèbes by former French intelligence officer André Achiary and members of the Union Française Nord-Africaine, (Union of French North Africa) which killed seventy-three local Arab residents. Just ten days after the Rue de Thèbes attack, the FLN, urged on by Ramdane Abane, adopted an explicit policy of indiscriminate terrorism at the Soummam Conference. Zohra Drif recalled:

“Before Rue de Thèbes, neither the FLN nor ALN had any bombs, explosive labs, specialists in the explosives field, or activists prepared to place bombs in public places… [O]ur bombings were a response – completely necessary but not premeditated – to the bomb attacks perpetrated by European civilians against our people.”

Martha Crenshaw has noted how in the Algerian War of Independence, the term engrenage — literally “the engaging of gears” — was used to emphasize the self-perpetuating nature of the conflict. It’s an apposite image.

Systemic police brutality is often cited in personal histories as a radicalizing factor. Dieter Kunzelmann, one of the leaders of Tupamaros West Berlin who was jailed for five years in the early 1970s for terrorism-related offenses, recalled in an interview with the BBC that it was the experience of routine police violence that pushed him and many of his comrades into taking up arms: “The debate over violence in the anti-authoritarian movement which led to armed resistance in the urban guerrilla movement was a result of us getting beaten up such a lot [by the police]. That goes without saying.” His observation was echoed by the RAF’s Horst Mahler: “We marched in the streets against the genocide in Vietnam with the belief that we were doing the best thing in the world. Then, there was the massive aggression of the state apparatus, and there was one death [of the student Benno Ohnesorg].” Michael Baumann also described the impact Ohnesorg’s death had on him: “Benno Ohnesorg. It did a crazy thing to me. Whenhis casket went by, it just went ding, something got started there.” Baumann joined Bewegung 2 Juni (2nd June Movement), an anarchist terrorist group formed in direct response to Ohnesorg’s death that took the date of the incident as its name. An Italian militant active in the Movimento Comunista Rivoluzionario (Revolutionary Communist Movement, or MCR) also blamed aggressive police tactics for escalating tensions between left-wing protestors and the ruling establishment in same period:

“It is first of all a problem of suffered violence. The first images are linked to the police charges. The first strong signs of an unsustainable situation, a situation which really had to be changed, comes those years from Avola and
Battipaglia. They came from those demonstrations, by the way not student ones, that were hit and repressed, with the death of people who had demonstrated.”

For November 17 member Patroklos Tselentis, it was the violent suppression by the Greek authorities of a student demonstration in 1980 that made the critical difference: “The events at the Polytechnic had a radicalizing effect on me. I was lucky not to have been hurt in the clashes, but many friends of mine, and many friends of theirs, sustained serious injuries at the hands of the police.” Likewise, Carlos Marighela’s ALN October Revolutionary Group declared in September 1969: “Finally, here is a warning to those who torture, beat and kill our comrades. We shall not allow these atrocities to continue. This is a last warning. Anyone who persists should beware. Now it is an eye for an eye and a tooth for a tooth.”

The experience of being detained, or of seeing a loved one detained, especially if that detention seems unjust, is also a commonly reported radicalizing experience. Nicos Sampson was one of EOKA’s leading operatives and by January 1957, he was said to have participated in at least twenty-five murders and attempted murders. However, he didn’t start out as a hardened criminal or street thug: “I was the best reporter in Cyprus when the police arrested me in Famagusta. I was innocent. I was sent to prison for three months on a false charge and when I came out I began working for EOKA.”

Likewise, Carlos Marighela’s ALN October Revolutionary Group declared in September 1969: “Finally, here is a warning to those who torture, beat and kill our comrades. We shall not allow these atrocities to continue. This is a last warning. Anyone who persists should beware. Now it is an eye for an eye and a tooth for a tooth.”

The Northern Ireland conflict abounds with stories of personal outrage, loss, and radicalization. The hunger striker Bobby Sands wrote that his nationalist sentiments had become aroused after watching a unionist mob ambush a Catholic civil rights march at Burntollet Bridge, with apparent police connivance, commenting: “That imprinted itself in my mind like a scar, and for the first time I took a real interest in what was going on. I became angry.”

Tony Doherty was just nine-years-old when his father, Patrick, was shot dead by British paratroopers in Londonderry/Derry on Bloody Sunday in 1972. Patrick Doherty had been a steward on the march. In 1981, Tony joined the Provisional IRA. When first asked by a PIRA recruiter his motivation for joining, his answer was unequivocal: “I wanted to get revenge for the death of my father.” Within a year, he had been arrested in possession of explosives while planning to bomb a British government building. He was sentenced to eight years in prison. A senior member of Provisional IRA told the psychologist John Horgan: “For me anyway, the sight of
the B Specials and the Royal Ulster Constabulary beating nationalist people off the street in Derry was a big factor in joining the republican movement.” PIRA veteran Anthony McIntyre explained: “Why did I become involved in the IRA? It was because of a process of British state repression as clearly distinct from any sort of attachment to republican ideology.” Another former PIRA man told the researcher Richard English that one reason he joined the Provisionals was that he came from a republican family but then added:

“Another reason — and this cannot, cannot be overestimated — was, when the troubles did break out, the reaction of the security forces within the nationalist areas … So those are basically the two reasons, and mostly I would say the latter — to strike back at what was going on in those districts.”

Seán MacStiofáin, the first Chief of Staff of the Provisional IRA, once reflected on the early years of the conflict with the observation, “it has been said that most revolutions are not caused by revolutionaries in the first place, but by the stupidity and brutality of governments. Well, you had that to start with in the north all right.”

The Palestinian experience is little different. Hamas co-founder Dr. Abdel Aziz al-Rantisi lost his uncle, grandfather, and three cousins to fighting with the Israelis. He told the terrorism researcher Mark Juergensmeyer that the suicide bombings carried out by Hamas were intended to make Israelis feel the same pain they had inflicted on Palestinians: “We want to do the same to Israel as they have done to us... It is important for you to understand that we are the victims in this struggle not the cause of it.” Al-Rantisi recalled that his group had initially restricted its attacks to Israeli military personnel and only extended its attacks to encompass civilian targets after the massacre perpetrated at Hebron’s Tomb of the Patriarchs by Dr. Baruch Goldstein in February 1994. Another senior Hamas figure, Imad Faluji, also commented on the same incident: “The Israelis killed our women and children during the holy month of Ramadan, we wanted to do the same to Israel, to show them that even their women and children are vulnerable — none are innocent.” After the killing of senior Hamas member Salah Shehada in a July 2002 Israeli air strike that also claimed the lives of thirteen members of his extended family including several children, al-Rantisi issued a statement in which he warned: “There will be no peace initiative after today. We will chase them in their houses and in their apartments, the same way they have destroyed our houses and our apartments.” Little over a week later, a Hamas operative left a bomb in a cafeteria on the campus of Jerusalem’s Hebrew University, which exploded without warning killing nine students and staff, and injuring 100 more. At a Hamas rally in Gaza City celebrating the attack, one speaker told the crowd: “We give this gift to the soul of Sheikh Salah Shehada and we say to the al Qassam Brigades we are waiting for more.” Commenting on the attack, a senior Hamas official, Ismail Haniyeh, told the Los Angeles Times: “If [the Israelis] are going to attack our children, then they will have to expect to drink from the same poison.”

One particularly emblematic Palestinian case is that of Hanadi Jaradat, a twenty-nine-year-old lawyer from the Palestinian West Bank town of Jenin, who blew herself up in a restaurant in Haifa in October 2003 killing twenty-one people and injuring fifty-one others. Her fiancé had been killed by the Israeli Defense Forces in 1997, and in June 2003, both her brother and cousin had also been killed during a raid by an undercover unit from the Israeli Border Police. The cousin had been a senior member of Palestinian Islamic Jihad (PIJ) and was a wanted fugitive, but Israeli sources could not agree on whether her brother was an active member of PIJ or not. The Jordanian newspaper Al Arab al-Yum reported that, in her eulogy for the two men, Hanadi vowed that their blood would not be shed in vain: “The murderer will yet pay the price and we will not be the only ones who are crying ... If our nation cannot realize its dream and the goals of the victims, and live in freedom and dignity, then let the whole world be erased.” Hanadi’s father, Taisir, told the Al Jazeera television network:
“My daughter’s action reflected the anger that every Palestinian feels at the occupation. The occupation did not have mercy on my son Fadi, her brother. They killed him even though he was not a wanted person, they murdered him in cold blood before Hanadi’s eyes, I will accept only congratulations for what she did. This was a gift she gave me, the homeland and the Palestinian people. Therefore, I am not crying for her. Even though the most precious thing has been taken from me.”

PIJ claimed responsibility for the attack in Haifa, and the cycle of violence continued when two weeks afterwards the IDF arrived to demolish the Jaradat family’s home. Hanadi was the eldest of nine children. Another former Head of Shin Bet, Yaakov Peri, admitted: “The Intifada stirred in many young persons a desire to take revenge of the Israeli authorities for a long list of issues: prolonged detention in difficult conditions, the loss of a family member or a close friend in one of the clashes, humiliating conduct during a search and much more.”

Finally, the transnational Islamist movement inspired, and to a certain extent led, by al-Qaeda and ISIL throws up many familiar narratives of suffering and revenge. Montassir al-Zayyat, Ayman al-Zawahiri’s biographer, maintains that it was “the traumatic experience suffered by Zawahiri in prison [that] transformed him from being a relatively moderate force in al-Jihad into a violent and implacable extremist.” The current Head of al-Qaeda was detained in Egypt in 1981 following the assassination of Anwar Sadat and jailed until 1985 during which period he was, by his own account, subjected to coercive interrogation methods by the Egyptian security forces: “There they kicked us, they beat us, they whipped us with electric cables, they shocked us with electricity... And they used the wild dogs... And they hung us over the edges of the doors with our hands tied at the back!”

Al-Qaeda in the Arabian Peninsula (AQAP) bombmaker Ibrahim al-Asiri likewise told an interviewer that he turned against the Saudi state after he was interdicted and imprisoned while trying to make his way to Iraq to join the insurgency against US forces: “They put me in prison and I began to see the depths of [the Saudi] servitude to the Crusaders and their hatred for the true worshippers of God, from the way they interrogated me.”

Sajida al-Rishawi, an aspirant suicide bomber recruited by Abu Musab al-Zarqawi to take part in the November 2005 Amman hotel bombings, had lost two brothers and a brother-in-law to US forces in Iraq. Al-Rishawi took part in the attack at the Radisson Hotel, but her suicide vest failed to go off and she fled the scene. When she was captured by the Jordanian authorities two days later, she told her interrogator: “They told me I would be killing Americans. All I wanted was to avenge the deaths of my brothers.”

But perhaps the most telling example of all comes in a videotaped speech broadcast by Al Jazeera in November 2004 in which Osama bin Laden explained why al-Qaeda had launched its operation against New York and Washington on 11 September 2001:

“Allah knows that it had never occurred to us to strike the towers. But after it became unbearable and we witnessed the oppression and tyranny of the American-Israeli coalition against our people in Palestine and Lebanon, it came to my mind. The events that affected my soul in a direct way started in 1982 when America permitted the Israelis to invade Lebanon and the American Sixth Fleet helped them in that. This bombardment began and many were killed and injured and others were terrorized and displaced. I couldn’t forget those moving scenes, blood and severed limbs, women and children sprawled everywhere. Houses destroyed along with their occupants and high rises demolished over their residents, rockets raining down on our home without mercy ... In those difficult moments many hard-to-describe ideas bubbled in my soul, but in the end they produced an intense feeling of rejection of tyranny,
and gave birth to a strong resolve to punish the oppressors. And as I looked at those demolished towers in Lebanon, it entered my mind that we should punish the oppressor in kind and that we should destroy towers in America in order that they taste some of what we tasted and so that they be deterred from killing our women and children.”

While individual stories and qualitative accounts are certainly persuasive, it is also worth noting that a number of quantitative studies have added further evidence of the damaging impact of state abuses. Mia Bloom has noted that there is “an empirical regularity” in Chechnya, Palestine, and Sri Lanka linking the loss of a family member to “unjust” state action and the choice to carry out an act of suicide terrorism. A study conducted for the US-based National Bureau of Economic Research on insurgent recruitment in Afghanistan in 2009–2010 found that revenge for the death of a loved one was often a crucial determining factor in an individual’s decision to join the insurgency. In 2014, the Institute for Security Studies in South Africa approached ninety-five Kenyan residents associated with the Somali terrorist group al-Shabaab in an attempt to find out why they had joined the organization. When asked “the single most important factor” that had pushed them to embrace violence, 65% of those approached referenced the Kenyan government’s aggressive counter-terrorism strategy towards Kenyan Muslims and Kenyans of Somali descent, specifically citing the assassination of Muslim leaders, collective punishment, arbitrary arrest, and police beatings among their complaints. A February 2017 survey conducted in North East Nigeria by the Network for Religious and Traditional Peacemakers found that 57% of former Boko Haram fighters interviewed by the researchers identified a desire for revenge as having had a major influence on their decision to join Boko Haram. One former Boko Haram member told the researchers that security forces “kill innocent people that are not members... I think they deliberately do so. So [people] join the group to fight the military.” Further support for these findings came from a transnational United Nations Development Programme study, Journey to Extremism in Africa, which interviewed 495 current and former African militants and found that 71% cited government action, including the “killing of a family member or friend” or the “arrest of a family member or friend,” as the tipping point that prompted them to join a terrorist group. The authors concluded that state security-actor conduct should therefore be considered “a prominent accelerator of recruitment, rather than the reverse.”

A key finding of quantitative studies into the putative relationship between poverty and terrorism conducted in the decade after the 9/11 attacks was that while poverty did not correlate in absolute terms to an increase in terrorism, human rights abuses and the suppression of civil liberties did. Jitka Malečková found that at a given level of income, countries with a low Freedom House Index score for civil liberties were consistently more likely to produce international terrorists. Similarly, a cross-national empirical study conducted by James Walsh and James Piazza found that countries with a poor human rights record were also more likely to experience both domestic and transnational terrorist attacks. A third study carried out by Freedom House itself found that between 1999 and 2003, 70% of all deaths from terrorist attacks were caused by terrorist groups originating from countries characterized by the organization as “Not Free.” This has proved to be the one consistent takeaway common to most such studies into the causes of terrorism. A number of influential researchers working in this field have reached similar conclusions, including Ethan Bueno de Mesquita, James Fearon, Douglas Hibbs, Alan Krueger, David Laitin, Mark Lichbach, and Michael Mazarr.

In fairness, it must be emphasized again that just as not every son of a Basque joins ETA, not every abused individual becomes a terrorist, nor equally has every terrorist necessarily suffered personally from human rights abuses at the hands of the state. It is simply a common, perhaps the most common feature, of radicalization case studies. However, of further concern to counter-terrorism officials should be the fact that such experiences can also serve to amplify
some of the other principal drivers of violent extremism enumerated above. As in the example of Udham Singh, it is easy to see how taking on the role of an avenger, especially on behalf of one’s community, could add substance to an individual’s quest for personal significance. It is equally easy to see how such abuses might provoke empathy for the abused in others. Chérif Kouachi, one of the two brothers behind the attack on the offices of the French satirical magazine *Charlie Hebdo* in January 2015 in which twelve people were killed, told a reporter who contacted him during his fatal stand-off with French police: “It was everything I saw on the television, the torture at Abu Ghraib prison, all that, which motivated me.” The centrality of kinship and friendship networks to the makeup of terrorist groups adds a personal dimension to the aftermath of kinetic state action against them, ensuring the cycle of violence is likely to continue. As Gregory Johnsen has noted, pursuing a policy of targeted assassination in a country like Yemen with a deep tribal commitment to *thar* (revenge) or Afghanistan where the strict *Pashtunwali* code of honor requires a wronged party to seek *badal* (variously translated as revenge or justice) is only likely to prolong conflict. A sense of social exclusion is only likely to be exacerbated by the application of overly aggressive and intrusive tactics. The Belfast-based criminologist Paddy Hillyard coined the term “suspect communities” to describe how the wider Catholic community in Northern Ireland had come to be treated very differently from the rest of the population in law, policy, and police practices. Floris Vermeulen, who has studied European attempts to engage resident Muslim communities over the past decade, has similarly warned that by conflating the threat posed by a small minority of radicalized extremists with entire communities, rather than the select few, local authorities risk prescribing public policy solutions that miss their intended target, alienate natural allies, and create suspect communities who, isolated from the authorities, are much less likely to push back against the extremists in their midst. One Somali refugee summed up the disconnect perfectly in a conversation with the counter-extremism researchers Heidi Ellis and Saida Abdi: “They feel I am a threat, but I feel I am a target.” If they are to have any chance of success, community engagement programs must be perceived as something that is being done in partnership with communities, rather than imposed on them.

This is where international human rights law comes in. A commitment to observing international human rights norms can prevent states from adopting counter-terrorism tactics that play straight into the hands of terrorist strategists, and give alienated members of society further reason to consider violent extremism as a pathway to change. Supporters of a more muscular counter-terrorism approach, true believers in the necessity of turning to “the dark side,” typically advance variants of the argument that human rights protections tie counter-terrorism’s hands, accompanied by emotionally charged appeals to intuition rather than evidence. The Israeli Prime Minister Benjamin Netanyahu’s observation that “if [democratic governments] do not fight terrorism with the means available to them, they endanger their citizenry” is typical of this approach. If they can throw in dash of swaggering machismo to underscore the point, so much the better. Taking charge of the Palestine Police Force amidst the Arab Revolt in 1937 the veteran colonial policeman Sir Charles Tegart and his deputy Sir David Petrie described their ideal recruit as a “tough type of man, not necessarily literate, who knows as much of the game as the other side.” Sixty-five years later the former Head of the CIA’s Clandestine Service, Jose Rodriguez, was likewise true to type when he told the reporter Lesley Stahl: “We needed to get everybody in government to put their big boy pants on and provide the authorities that we needed [to go after the terrorists].” However, it is worth taking a moment to measure these assertions against the reality in the field. International human rights law and international humanitarian law provide a framework within which lawful state responses to terrorism should be conducted. This framework makes provision for wide-ranging international cooperation on counter-terrorism, establishes the benchmarks that characterize genuinely democratic societies, and creates an international regime of protection for fundamental human rights — such as the right to life, the right to
liberty, the right to freedom of conscience, and the right to privacy — to ensure that individuals enjoy a measure of protection from the unbridled power of the state. Executive powers are limited for the most part by the requirement that due process is observed in their application and that they are used in a manner that is reasonable, necessary and proportionate to the threat posed by criminal activity. International law recognizes that, on rare occasions, grave circumstances may arise which may require the temporary suspension of some protected rights — it simply requires that any such suspension must be done in a lawful manner and that state reverts to the status quo ante — full rights observance - at the earliest practical opportunity. At both the individual and the national level, the right to defend oneself in the face of attack is accorded particular prominence. In reality, international law accords state considerable latitude in responding to terrorist threats. However, it does also establish some fundamental red lines that states cannot cross in any circumstances. For example, states cannot detain suspects indefinitely without trial, states cannot torture suspects or render them to be tortured, and states cannot murder suspects with impunity. Any deviation from the “fundamental principles of fair trial” — including the presumption that a suspect is innocent until proven guilty — is completely prohibited.\textsuperscript{182} Freedom from discrimination is also regarded to be an absolute human right.\textsuperscript{183} Indeed, the United Nations General Assembly has also identified “ethnic, national and religious discrimination” as one of the “conditions conducive to the spread of terrorism.”\textsuperscript{184} So, the question now arises if it is possible to mount an effective response to terrorism without crossing these red lines, and moreover whether crossing any of these redlines has ever proved to be a remotely productive counter-terrorism tactic.

International human rights law anticipates that states will need to surveil, eavesdrop on and otherwise clandestinely collect information on the person and activities of terrorist actors using skilled surveillance professionals, technical devices, covert searches, informants, and undercover officers. Navi Pillay, the former UN High Commissioner for Human Rights, purposely acknowledged the vital role that intelligence collection plays in the prevention of terrorist violence: “The use of accurate intelligence is indispensable to preventing terrorist acts and bringing individuals suspected of terrorist activity to justice.”\textsuperscript{185} The Council of Europe’s Committee of Experts on Special Investigation Techniques in relation to Acts of Terrorism has likewise noted:

“The objective of the European Convention on Human Rights is not to disarm the authorities responsible for prevention or prosecution in criminal matters. The Convention sets out criteria in order that the authorities’ activities should constantly be guided by the rule of law and the pursuit of the democratic ideal.”\textsuperscript{186}

In fact, Special Investigation Techniques are limited in their use for the most part only by the requirement that they are defined in law, that due process is observed in their application, and that they are used in a manner that is reasonable, necessary and proportionate to the threat posed by criminal activity in question. There is a growing body of international jurisprudence that delineates where the line between proportionate and disproportionate action should be drawn. The only other major restriction is that in deception operations where a criminal actor is fooled into dealing with undercover operatives, those operatives cannot act to commission or instigate the offence. International human rights law does not allow for the use of agent provocateurs. When a person who would not otherwise be predisposed to commit an offence is encouraged to do so by a government official this is considered to be entrapment. The tests set by international human rights law for the use of Special Investigative Techniques go to the heart of the dilemma facing all national security actors operating within democratic systems — how does one protect the public while also protecting the rights and freedoms they enjoy. There is little point adopting policies that ultimately undermine the institutions they are
supposed to protect. As a bumper sticker popular in the United States declaims: Freedom isn’t free. Some risk is inevitably involved in living in a free society. The challenge is to get the balance right, to ensure, in the words of the current Director General of the British Security Service, Andrew Parker, that being on the authorities’ radar is not the same as being under their microscope.187

Perhaps the investigative activity that has received the most attention from both human rights advocates and national security hawks since the September 11th attacks is the interviewing of terrorist suspects, and specifically the use of coercive measures by the interviewers. The potential to question a terrorist suspect obviously represents an important information-gathering opportunity. There is unquestionably great value to a cooperating suspect who is prepared to provide answers to his interlocutors’ questions openly, honestly, and to the best of his or her ability. But there is a universe of difference between rapport-based conversations and coerced speech. The simple fact is that both can result in the production of truthful or deceptive statements. However, it is important to understand that any testimony obtained only represents one stage of any competent investigation, and, until such testimony is tested, analyzed, and compared to other relevant evidence or intelligence, the wise investigator is going to place very little store in it. History is replete with examples of hardened terrorists who have ended up cooperating with the authorities in rights-based police interviews. The Norwegian right-wing extremist mass murderer Andreas Behring Breivik and Osama bin Laden’s former driver Salim Hamdan are both examples of cooperative interview subjects. Equally, there are many well-documented examples of motivated terrorists successfully either protecting their secrets or proffered false or misleading information to their torturers. Ibn al-Shaykh al-Libi, the former emir of al-Qaeda’s al Khaldan training camp, and Khaled Sheikh Mohammed, architect of the September 11th attacks, both succeeded in fooling their interrogators despite suffering horrific abuse. However, while the record shows that neither approach can guarantee a suspect’s full and honest cooperation, the unlawful use of coercive methods comes with a host of both legal and utilitarian downsides, not least the vulnerability of this approach to confirmation bias, the not uncommon concomitant risk of torturing an innocent individual, the personal criminal liability of the torturer (torture is an international crime with no statute of limitations), and the catastrophic damage to the reputation of the state that allows such methods. Former CENTCOM Commander and Director of the CIA David Petraeus, ruefully acknowledged: “Abu Ghraib and other situations like that are non-biodegradable. They don’t go away. The enemy continues to beat you with them like a stick.”188 So, when a politician with little or no national security experience like Donald Trump says, as he did at a campaign event in New Hampshire in February 2016, that “[waterboarding] is fine, and much tougher than that is fine. When we're with these animals, we can't be soft and weak, like our politicians,”189 it is worth remembering that the FLN Commander Saadi Yacef once said of France’s unrestrained use of torture in Algeria and its torturer-in-chief, Paul Aussaresses: “Actually torture helped the FLN enormously because what it did was expose the real face of the French military.... you could say that Aussaresses was one of the FLN’s most important assets because the more he tortured, the more militants we recruited.”190

The avowed purpose of most counter-terrorism investigations is the arrest, conviction and subsequent incarceration of suspected terrorists, and international human rights law offers many different frameworks within which a state may detain a terrorist suspect or convicted terrorist: administrative detention, pre-trial detention, punitive detention, and the confinement of prisoners of war. The fundamental principle governing all these forms of detention is that that “no one shall be subjected to arbitrary arrest or detention” or “deprived of his liberty except on such grounds and in accordance with such procedure as are established by law.”191 The drafters of the International Covenant on Civil and Political Rights made it clear in their preparatory work that “arbitrariness” should not simply be equated with “unlawful” but should rather be interpreted more broadly “to include elements of inappropriateness, injustice, lack of
predictability, and due process of law.” No derogation from the customary international law prohibition on arbitrary detention is possible. Secret detention and enforced disappearance, practices closely associated with torture, are similarly prohibited and may, if used in a widespread or systematic manner, amount to crimes against humanity. It is difficult to imagine a compelling argument that these basic principles present an obstacle to successful counter-terrorism operations. Although arbitrary detention has a long and ignoble history one does not have to look further than the CIA’s discredited Black Site programme, forensically exposed by Senate Select Intelligence Committee investigators, for a simple cost benefit analysis of the value of such an approach. The Black Sites were associated with torture, produced little or no actionable intelligence, resulted in the enforced disappearance of a completely innocent German national, Khaled el-Masri, which the CIA tried to cover up, placed allies like former Head of Polish Intelligence, Zbigniew Siemiaikowski, in legal jeopardy, and impacted intelligence-sharing with close partners like the United Kingdom, with a Director General of MI5, Dame Eliza Manningham-Buller, publicly acknowledging that the British government had “greater inhibitions than we once did” in sharing intelligence the United States. The brutal leader of al-Qaeda in Iraq Abu Mus’ab al-Zarqawi was quick to take advantage of the publicized abuse of US detainees in a communiqué entitled Our Shari’a Stance with Regard to the Government of the Iraqi Karzai, commenting: “I do not think that any intelligent person remains who believes in the monstrous lie of promised democracy after the revelations of Abu Ghraib and the joke of Guantanamo.” It is hard to argue that his observation lacked merit.

The last of the four main categories of executive action is the use of force. Force is an extremely broad concept in international law, with lawful forms of compulsion extending from the verbal notice of arrest and minimal physical restraint at one end of the spectrum, to the use of potentially lethal weapons at the other. As with other areas of executive action, international human rights law imposes two core obligations on officials who are lawfully empowered to use force in performance of their duties — that force is used only when it is necessary to do so, and that, when it is used, it is used in a manner strictly proportionate to the seriousness of the offence and the legitimate objectives sought. The requirement of necessity also imposes an obligation to minimize the level of force applied “regardless of the level of force that would be proportionate.” It is not the gravity of the threat that determines the level of force that can be used to contain it, but rather the manner of action that would be sufficient to neutralize the threat. The criterion that there should be a proportionate relationship between the degree of force used and the legitimate objective for which it is being used, requires that any escalation of force ceases when the consequences of applying additional force outweigh the value of the objective for which it is being employed. In sum, international human rights law imposes limits to ensure that force is used as sparingly as possible, but also recognizes that sometimes the only way to protect the public from acts of violence is to meet force with force.

If we look at states that have gone beyond these lawful limits to embrace what is termed targeted killing in modern vernacular, they have frequently had cause to regret it. First, there is the potential for mistaken identity, as in the case of Mossad’s July 1973 murder of an innocent Moroccan waiter called Ahmed Bouchiki in Lillehammer, Norway, who was erroneously and inexplicably identified the Black September Organization’s operations chief, Ali Hassan Salameh. One senior Mossad officer later excused the error with the telling admission: “Our blood was boiling. When there was information implicating someone, we didn’t inspect it with a magnifying glass.” Then there is the issue of collateral damage, Mossad finally settled its score with Salameh in January 1979 killing him, along with his bodyguards, with a car bomb in Beirut, but in doing so also killed four innocent bystanders, including a German nun and an English student. In April 2015 President Obama apologized for a US drone strike in Pakistan which accidentally killed two western hostages, Warren Weinstein and Giovanni Lo Porto, held by al-Qaeda. This admission prompted a powerfully
memorable headline on Public Radio International: “If Obama apologized for 1 civilian drone victim every day, it would take him 3 years.”

Grounded in extensive research by the Bureau of Investigative Journalism into the use of drones in counter-terrorism operations, this genuinely shocking statistic graphically underscores just how callous and unrestrained American use of force has become. And finally there are the unintended consequences of striking out, a killing can precipitate deeper conflict, as in the case of the murder of Boko Haram founder Mohammed Yusuf in Nigerian police custody in July 2009, which gave birth to a terrorist insurgency that endures in North East Nigeria to this day, or the Israeli February 1992 Apache helicopter strike on the Secretary-General and co-founder of Hezbollah, Sheikh Abbas al-Musawi, which a month later led to Hezbollah detonating a truck packed with explosives outside the Israeli Embassy in Buenos Aires killing twenty-nine people and wounding 240. In 2006, the US National Intelligence Estimate predicted that the loss of key leaders like Osama bin Laden and Abu Musab al-Zarqawi would cause [al-Qaeda] to fracture into smaller groups. Both men are now long dead, killed by US forces, and, as the Estimate predicted, al-Qaeda and al-Qaeda in Iraq were significantly degraded by these and other losses. But, the space left by al-Qaeda’s decline was quickly filled by a still more violent and destructive foe: ISIL. The underlying political appeal of Islamist extremism to an angry and alienated minority had changed very little. As another former Director of the CIA, General Michael Hayden, has noted, there are always second and third order effects of covert action and these can be very difficult to predict. Before reaching for the hammer in the tool box, it is worth remembering another of David Fromkin’s pithy warnings: “Terrorism can… make heroes out of gunmen, and thereby rally popular support to the cause… Just as it can make gangsters into heroes, terrorist provocations can also make policemen into villains.”

Conclusion

The facts should really speak for themselves: terrorists see advantage in provoking the state into overreacting and abusing human rights; social science research has identified state abuses as a major – perhaps the major – driver of terrorist recruitment; international human rights law anticipates and endorses the lawful use of a wide range of potentially intrusive and robust enforcement tools, it simply places limits on the use of these tools so that they are not abused and their use does not undermine democratic life; the historical record strongly suggests that exceeding these limits serves little practical purpose, but can greatly damage the societies that do so. The synergy between human rights observance and effective counter-terrorism should be obvious to any competent national security professional. And yet, state after state ignores these facts and repeats the mistakes of its forebears, so much so in fact that a December 2015 Gallup poll found that 51% of Americans questioned were “very worried” or “somewhat worried” that either they or a family member could become a victim of terrorism, which, in a country of 330 million people that has lost approximately 213 people to a more or less even mix of Islamist and far-right terrorism in the eighteen years since the
September 11th attacks, is patently absurd. This is an area in which a little bit of tough talk from the would-be hard men of the national security community might actually be appropriate, and perhaps even helpful. If we want to keep our societies safe, we need to reinforce the resolve and emotional resilience of our people. Terrorism is not, on its own terms, an existential threat, nor is it an especially present one. Terrorism does exist, it is a problem, and like other manifestations of violent crime, it is entirely appropriate that states take every lawful precaution to prevent terrorist incidents. Indeed, states have a human rights obligation to do so—both to protect the lives of their citizens, and to ensure the full enjoyment of their human rights. It makes absolutely no sense to jeopardize those rights in the process, to destroy the village in order to save it. Terrorism only represents an existential threat if we make it one.

Terrorism has been with us for more than 150 years and it isn’t going away any time soon. The bomber will sometimes get through. Just like other forms of criminal activity it is unrealistic to expect that extremist violence can be eliminated completely. Not every terrorist attack is preventable, and the reality is that when opportunities to prevent attacks are missed, this typically reflects a failure of competency, imagination, or capacity on the part of the authorities, rather than an institutional shortfall in investigatory powers. Intelligence and security agencies are not infallible, and it is unrealistic to expect them to be so. As Eliza Manningham-Buller admitted while Director General of MI5, intelligence services face acute and very difficult choices of prioritization. It is not an easy job. More intrusive powers will not prevent every attack and most likely would just generate additional intelligence clutter further obscuring the needle represented by terrorist activity in a giant haystack of irrelevant data. In the intelligence business, less is often more, intelligence-driven investigation is efficient, data-driven investigation for the most part is not. Former CIA Director David Petraeus admitted as much in an interview in May 2016: “Now the challenge, actually, is the amount of data we have; Big data has become overwhelmingly big.” Furthermore, as we have seen above, more intrusive powers may just make the situation worse by pouring more fuel on the fire. Once again, Fromkin got it right, the smart strategy is to avoid the terrorist trap altogether:

“The important point is that the choice is yours. That is the ultimate weakness of terrorism strategy. It means that, though terrorism cannot always be prevented, it can always be defeated. You can always refuse to do what they want you to do… So, if you can do so, you should accept the consequences, however terrible, of standing firm in order to avoid an infinite sequence of painful events.”

As hard as it may be, we have to learn to live with some loss. The price of freedom is a certain degree of vulnerability.

Resisting pressure to abridge our laws and liberties in order to suppress terrorism takes political courage and principled leadership, which is often, but not always, in short supply, especially in times of crisis. It can be done, and every now and again a politician rises to the challenge. In his July 2011 National Memorial Address for the victims of Anders Behring Breivik’s shocking attack on Oslo and Utøya, Prime Minister Jens Stoltenberg told the Norwegian people: “I have been impressed by the dignity, compassion and resolve I have met. We are a small country, but a proud people… Our answer is more democracy, more openness and more humanity.” In December 2014, US Senator John McCain took to the Senate floor to commend the release of the Senate Select Committee on Intelligence’s report on the use of torture by the CIA, and deliver a powerful speech outlining what a truly robust democratic response to terrorism should look like:
“Our enemies act without conscience. We must not. This executive summary of the Committee's report makes clear that acting without conscience isn't necessary, it isn't even helpful, in winning this strange and long war we're fighting. We should be grateful to have that truth affirmed. Now, let us reassert the contrary proposition: that it is essential to our success in this war that we ask those who fight it for us to remember at all times that they are defending a sacred ideal of how nations should be governed and conduct their relations with others — even our enemies.”

This is what real resilience looks like. To defeat terrorism we need to hold true to our values, not jettison them at the first sign of trouble. We need to cherish and protect human rights, they were hard won and are all too easily lost. They are also the heart and soul of an effective counter-terrorism policy. What Jens Stoltenberg, John McCain, and David Fromkin all seem to have understood is this fundamental truth, that, in the final analysis, the war of the flea is actually all about the dog.

Tom Parker is the author of “Avoiding the Terrorist Trap: Why Respecting Human Rights is the Key to Defeating Terrorism” (2019). He was until recently the Chief of Party of a European Union project providing assistance to the Office of the National Security Adviser in Baghdad, Iraq, and is currently providing advice to the Nigerian government. Tom has previously served as an adviser on human rights and counter-terrorism to United Nations Counter-Terrorism Implementation Task Force (CTITF) and was one of the principal authors of the UN’s Preventing Violent Extremism Plan of Action. He has also worked as the Policy Director for Terrorism, Counterterrorism and Human Rights for Amnesty International USA, as a war crimes investigator for the United Nations International Criminal Tribunal for the former Yugoslavia (ICTY) working in the field in Bosnia and Kosovo, and as an Intelligence Officer in the British Security Service (MI5). Tom has taught undergraduate and postgraduate courses on international terrorism in Yale University’s Residential College Seminar Program, Bard College’s Globalization and International Affairs Program, and the National Defense University at Fort Bragg.
Endnotes

1 Tom Parker is the author of *Avoiding the Terrorist Trap: Why Respect for Human Rights is the Key to Defeating Terrorism*, and selected passages from the book appear here with the kind permission of World Scientific Press.


6 Ibid, p. 687.

7 Ibid, p. 688. See also McCauley, Clark, ‘Jujitsu Politics: Terrorism and Responses to Terrorism’; in: Kimmel, Paul and Stout, Chris (eds.), *Collateral Damage: The Psychological Consequences of America’s War on Terrorism*. Praeger Publishers, 2006


37 Grivas-Dighenis, George, *supra* note 36, p. 15.


41 Ibid, p. 118 and p. 123.

42 Ibid, p. 122.

43 Ibid, p. 123.


45 Fromkin, David, *supra* note 5, pp. 689-690.


48 Zirakzadeh, Cyrus, ‘From Revolutionary Dreams to Organizational Fragmentation: Disputes over Violence within ETA and Sendero Luminoso’; in: *Terrorism and Political*


53 Ibid, p. 100.


55 Ibid, p. 93.

56 Guevara, Ernesto, supra note 51.


58 Ibid.


60 Ibid, pp. 35–36.

61 Louise Richardson, supra note 4, p. 199.

62 Marighella, Carlos, supra note 59.

63 Ibid.

64 Sterling, Claire, supra note 49, p. 163.

65 Ibid, p. 38.

66 Ibid.

67 Ibid, p. 163.

68 Ibid, p. 162.


71 Ibid.

72 Meinhof, Ulrike, supra note 69, p. 368.


74 Iyad, Abu and Rouleau, Eric, supra note 17, p. 66.


76 Ibid, p. 120.

77 Ibid, p. 119.


80 Byman, Daniel, supra note 75, p. 365.
85 Thornton, Rod, *supra* note 83, p. 89.
89 Ibid. Since entering party politics Adams has consistently denied that he was an active member of the Provisional IRA but his role as a prominent early leader of the organization has been well documented, perhaps most notably by one of his closest allies during this period, former Belfast Brigade stalwart and senior republican Brendan Hughes.
99 Michael Ryan, *supra* note 97, p. 175.
100 Ibid, p. 159.
101 Ibid, p. 163.
104 Ibid.
105 Ibid.
106 Ibid.


115 Ibid, p. 1288.

116 Macintyre, Ben, ‘We can’t escape our bloody role in Sikh history’; in: *The Times*, 17 January 2014.


123 Ibid, p. 198.


125 Hoffman, Bruce, *supra* note 15, p. 161/1039


133 Della Porta, Donatella, *supra* note 131, p. 42.


135 Marighela, Carlos, *For the Liberation of Brazil*. The Pelican Latin American Library, 1974, p. 27.

137 Ibid, p. 63.
138 Miroff, Nick, ‘Do you know what it’s like to spend 20 years at war?’ in: Washington Post, 30 September 2016.
140 Sands, Bobby, ‘From a nationalist ghetto to the battlefield of H-Block’; in: An Phoblacht, 16 December 1978.
144 English, Richard, supra note 81, p. 123.
145 Ibid, pp. 122-123.
149 Ibid, p. 137.
152 Wilkinson, Tracy, ‘Blast Kills 7 at University in Jerusalem’; in: Los Angeles Times, 1 August 2002.
155 Ibid.
166 Ibid.
168 Ibid, p. 5.
Walsh, James and Piazza, James, ‘Why Respecting Physical Integrity Rights Reduces Terrorism’; in Comparative Political Studies, Vol. 43, No. 5, 2010.


Johnsen, Gregory, ‘How we lost Yemen’; in: Foreign Policy, 6 August 2013.


Vermeulen, Floris, supra note 175, pp. 287–288.

Ellis, Heidi and Abdi, Saida, supra note 177, p. 295.


Hoffman, Bruce, supra note 15, p. 124/1039.


Human Rights Committee, General Comment No. 32, Article 14: Right to equality before courts and tribunals and to a fair trial, U.N. Doc. CCPR/C/GC/32, 2007, Sec. I.


Council of Europe, Terrorism: Special Investigation Techniques, April 2005, p. 27.
Address by the Director General of the Security Service, Andrew Parker, to the Royal United Services Institute (RUSI), Whitehall, 8 October 2013.


‘The Latest: Clinton Vows to 'Make a Difference' Every Day’, Associated Press, 8 February 2016.

German, Mike, supra note 90, p. 119.

Article 9, International Covenant on Civil and Political Rights (ICCPR)


Joint Study on Global Practices in Relation to Secret Detention in the Context of Countering Terrorism of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin; the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, Manfred Nowak; the Working Group on Arbitrary Detention; and the Working Group on Enforced and Involuntary Disappearances, A/HRC/13/42, 19 February 2010, p. 2.

United States Senate Select Committee on Intelligence, Study of the Central Intelligence Agency's Detention and Interrogation Program, December 2014


Note by the Secretary General: Extrajudicial, summary or arbitrary executions, 5 September 2006, A/61/311, para 42.

Ibid, para 41.

Ibid, para 42.

Byman, Daniel, supra note 75, p. 53.


Jackson, Allison, ‘If Obama apologized for 1 civilian drone victim every day, it would take him 3 years’, Public Radio International. Available at: https://www.pri.org/stories/if-obama-apologized-1-civilian-drone-victim-every-day-it-would-take-him-3-years.

https://www.thebureauinvestigates.com/projects/drone-war


Fromkin, David, supra note 5, pp. 686-687.

Louise Richardson, supra note 4, p. 234.


Eliza Manningham-Buller, *The International Terrorist Threat to the UK: Speech by the Director General of the Security Service*, Queen Mary’s College, 9 November 2006.


Ibid.


Bibliography


Brooks, Rosa, ‘The Threat Is Already Inside: And nine other truths about terrorism nobody wants to hear’, Foreign Policy, 20 November 2015.


Council of Europe, Terrorism: Special Investigation Techniques, April 2005.


Joint Study on Global Practices in Relation to Secret Detention in the Context of Countering Terrorism of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin; the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, Manfred Nowak; the Working Group on Arbitrary Detention; and the Working Group on Enforced and Involuntary Disappearances, A/HRC/13/42, 19 February 2010.


Munoz, Michael, ‘Selling the Long War: Islamic State Propaganda after the Caliphate’ *CTC Sentinel*, November 2018.


Sands, Bobby, ‘From a nationalist ghetto to the battlefield of H-Block’, *An Phoblacht*, 16 December 1978.


United States, Senate, Select Committee on Intelligence, *Study of the Central Intelligence Agency's Detention and Interrogation Program*, December 2014.


Web-based Resources

The Bureau of Investigative Journalism, Shadow Wars. Available at: https://www.thebureauinvestigates.com/projects/shadow-wars

Combating Terrorism Center at West Point. Available at: https://ctc.usma.edu/

Council of Europe, Commissioner for Human Rights. Available at: https://www.coe.int/en/web/commissioner/thematic-work/counter-terrorism

Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism (START). Available at: https://www.start.umd.edu/gtd/

Human Rights First, Never Torture campaign. Available at: https://www.humanrightsfirst.org/campaigns/never-torture


Organization for Security and Cooperation in Europe, Office for Democratic Institutions and Human Rights. Available at: https://www.osce.org/odihr/countering-terrorism

United Nations Office on Drugs and Crime (UNODC), Terrorism Prevention Branch. Available at: https://www.unodc.org/unodc/en/terrorism/

United Nations Office on Drugs and Crime (UNODC), Education for Justice University Module Series on Counter-Terrorism. Available at: https://www.unodc.org/e4j/en/tertiary/counter-terrorism.html

United Nations Office of Counter-Terrorism. Available at: https://www.un.org/counterterrorism/human-rights
Chapter 35

Conclusions: Terrorism Prevention – The UN Plan of Action (2015) and Beyond

Alex P. Schmid

This concluding chapter compares some of the findings and recommendations of the contributors of this Handbook with the observations and recommendations of the UN Plan of Action to Prevent Violent Extremism (reproduced in full in the Appendix to this chapter). There are various similarities, which will be highlighted in this chapter. It then compares the findings of the UN Plan of Action with findings based on the science of System Analysis and looks at statistical correlations of terrorism. In other words, the preventive measures presented in this volume and in the UN Plan of Action are based on solid foundations. If fully and universally implemented by all UN member states, the recommendations of the UN Plan of Action could go a long way to reduce the emergence of violent extremism and terrorism. Its ultimate success stands and falls with national implementation plans. However, many UN members States hesitate to implement its evidence-based findings on the prevention of terrorism, probably due to their undemocratic regimes. Finally, the chapter looks at a few of the regional and national plans of action and sketches the elements for a generic strategy for the prevention of terrorism.

Keywords: extremism, lessons learned, plan of action, prevention, strategy, terrorism, united nations
“too much of the focus of the past two decades has been on the symptoms of terrorism and that, going forward, more attention needs to be given to prevention. This involves addressing conditions that include poor governance, corruption, inequality, human rights abuses, marginalization, and exclusion. These factors are often due to or exacerbated by predatory and other government behavior. Terrorists exploit them to recruit and radicalize supporters, which then drives other forms of violence and conflict and fragility. Emphasizing prevention also means including a wide array of actors outside the law enforcement and broader security fields ....”

– Eric Rosand and Alastair Miller (2021)²

In the context of this Handbook, prevention is about avoiding unwanted and harmful future violence of a terrorist kind. Since the future is to a considerable extent unknowable, it is often assumption-based rather than evidence-based. However, to the extent that the past is prologue of the future and that history-based forecasts are grounded in empirical evidence of known causal chains rather than mere assumptions, a degree of prevention is possible. In addition, we not only have the past as yardstick to prepare prevention measures, but we also have the experience of countries with no or low levels of terrorism. This chapter used both types of evidence to make the case for better prevention and preparedness policies.

Benjamin Franklin’s advice from 1736, “An ounce of prevention is worth a pound of cure,” begs the question: what exactly goes into that ounce of prevention? Policy-makers, PVE practitioners, and researchers have come up with many answers – but often also with empty hands.³ Rather than deepening research into prevention, they have often widened it. Prevention, which was once thought to be a narrow task, has become a task assigned to many – but often without much guidance.

Anti-terrorism in the form of preventing and countering terrorism has traditionally been the task of national law enforcement and intelligence and security agencies. Since 9/11, with the American declaration of a Global War on Terror (GWOT), it expanded – first in the US and soon thereafter in more countries - to the armed forces. The increased securitization of anti-terrorism ended up in many countries in a “whole-of-government” approach. In recent years, preventing terrorism and countering violent extremism has been pushed beyond this to a “whole-of-society” approach. This means that various actors and institutions (e.g. mothers, families, youth, teachers, schools, social services, prison and probation officers, sport clubs, moderate Muslims, places of worship, academia, local communities, cities and local government, business, human rights, NGOs, and social media) have been encouraged or tasked in some countries to assume prevention functions as well as de-radicalization roles.⁴

Regional security actors (e.g., OSCE, NATO) and multi-purpose international organizations (e.g., EU and UN) have become involved. The UN is involved in an “All-of-UN” effort to promote its Prevention of Violent Extremism Plan of Action. Under-Secretary General V.I. Voronkov, heading the UN Counter-Terrorism Office (UNOCT) since 2017, is the main focal point in the UN system for Preventing and Countering Violent Extremism (PCVE). He chairs the UN Global Counter-Terrorism Coordination Compact Working Group on Preventing and Countering Violent Extremism Conducive to Terrorism, which by early 2020 included no fewer than 43 in-house UN entities as well as international partners. V.I. Voronkov’s office also serves as the secretariat to the UN Secretary-General’s High-Level Action Group on Preventing Violent Extremism, which provides strategic level guidance to the P/CVE work of the UN system. All this would seem to suggest that the issue of
extremism/terrorism prevention – which was already addressed in the four pillars of the UN Strategy against Terrorism from September 2006\textsuperscript{5} - has finally become mainstream – next to the traditional core tasks of the UN: peace, human rights and development.

UN Secretary-General Ban Ki-moon had first announced the new Plan of Action to Prevent Violent Extremism in December 2015 with these opening words:

“Violent extremism is an affront to the purposes and principles of the United Nations. It undermines peace and security, human rights and sustainable development. No country or region is immune from its impacts. The present Plan of Action to Prevent Violent Extremism considers and addresses violent extremism as, and when, conducive to terrorism.”\textsuperscript{6}

The Plan of Action was officially “welcomed” and “taken note of” by the UN General Assembly at a time when IS was at the height of its power, with tens of thousands of foreign fighters joining it. It was presented by the outgoing UN Secretary-General Ban Ki-moon, who in early 2015 had been persuaded by US President Obama to develop such an instrument.\textsuperscript{7} Its future soon passed into the hands of the UN Secretary General António Guterres and his Under-Secretary-General V.I. Voronkov, and, even more so, rests in the hands of individual UN member states. If fully and universally implemented by all 193 UN members, the recommendations of this Plan of Action could go a long way to inhibit the emergence of violent extremism and terrorism.

The Plan of Action consists of a series of recommendations for member states, regional organizations as well as UN entities. As explained in a study by Saferworld:

“The UN Secretary-General’s Plan of Action to Prevent Violent Extremism describes PVE as systematic preventive measures that directly address the drivers of violent extremism. Setting out the UN’s intention to take a practical and comprehensive approach to address these drivers, it put forward more than 70 recommendations for concerted action at global, regional and national levels.”\textsuperscript{8}

These seven substantive priority areas of the Plan of Action to Prevent Violent Extremism are:

1. dialogue and conflict prevention;
2. strengthening good governance, human rights and the rule of law;
3. engaging communities;
4. empowering youth;
5. gender equality and empowering women;
6. education, skill development and employment facilitation; and
7. strategic communications, the internet and social media.\textsuperscript{9}

At the time of this writing (June 2021), the UN Plan of Action to Prevent Violent Extremism is the closest thing in the real world we have to parallel the concerns and findings of the contributors of this Handbook.\textsuperscript{10} In fact, many of the recommendations of this UN Plan of Action come close, or are almost identical, to those proposed by contributors of this Handbook as will be shown below.

**The UN Plan of Action in the Light of Findings by the Contributors of this Handbook**

In the following section, we will compare some of the recommendations by the contributors of this volume with those of the UN Plan of Action, following the seven substantive priority areas
of the UN Plan (see Appendix of this chapter for complete text of the UN plan).

1. Dialogue and Conflict Prevention

In the UN Plan of Action, it is noted under point 30 that,

“Prolonged and unresolved conflicts tend to provide fertile ground for violent extremism, not only because of the suffering and lack of governance resulting from the conflict itself but also because such conflicts allow violent extremist groups to exploit deep-rooted grievances in order to garner support and seize territory and resources and control populations. Urgent measures must be taken to resolve protracted conflicts. Resolving these conflicts will undermine the impact of the insidious narratives of violent extremist groups. When prevention fails, our best strategy towards securing lasting peace and addressing violent extremism entails inclusive political solutions and accountability.”

This is in line with observations made by several contributors to this volume, notably by A. Schädel, H.-J. Giessmann, C. McCauley, and A.P. Schmid. In an important sense, conflict prevention is terrorism prevention. Schmid, in his Twelve Rules for Preventing and Countering Terrorism places this even at the top of his list: “Try to address the underlying conflict issues exploited by the terrorists and work towards a peaceful solution while not making substantive concessions to the terrorists themselves.”

Unfortunately, there are a growing number of conflicts that form breeding grounds for terrorism. While there were 37 state-based armed conflicts worldwide in 2005, their number has increased to 54 by 2019, including seven full-scale wars. The rise of armed conflicts has been particularly significant in Africa, where the increase in the same period was from eight to 25 conflicts.

In the present Handbook, Clark McCauley also stresses the importance of conflict prevention as terrorism prevention:

“The time to prevent terrorism is early in the escalation of intergroup conflict. (...) Politicide and terrorism emerge out of asymmetric conflicts - political conflicts with histories of action and reaction over time. It is these trajectories of conflict that must be understood to prevent and reduce the extremes of violence against civilians....”

Andreas Schädel and Hans-Joachim Giessmann, in turn, note that “that terrorism and its effective prevention can only be understood as part of a wider political conflict and in combination with the surrounding structural power relationships....” They plead for conflict transformation which

“… does not build interventions around the terrorist group as the only actor and violent perpetrator in a conflict but allows for a wider understanding of violent extremism and terrorism as the result of structural drivers (e.g. repression, inequality, poor governance, violations of human rights, discrimination, unemployment, foreign interventions), individual motivations (e.g., a sense of purpose, victimization, belonging, identity, acceptance, status, expected rewards, material enticements) and enabling factors (e.g. presence of radical mentors, access to radical communities and ideologies, access to weapons, lack of state presence, absence of family support).”
A. Schädel and H.-J. Giessmann also stress - despite the bleak human rights record of terrorist groups - the importance of dialogue with them and observe that “… the instruments of negotiations and dialogue, although still categorically refused by some terrorism scholars and policymakers, can prove valuable additions to existing approaches to terrorism prevention.”

Further findings by the authors of this Handbook paralleling those in the UN Secretary-General’s Plan of Action can also be found when it comes to the second substantive priority area.

2. Strengthening Good Governance, Human Rights and the Rule of Law

In his Plan of Action to the General Assembly, UN Secretary-General stressed under point 27:

“Violent extremism tends to thrive in an environment characterized by poor governance, democracy deficits, corruption and a culture of impunity for unlawful behavior engaged in by the State or its agents. When poor governance is combined with repressive policies and practices which violate human rights and the rule of law, the potency of the lure of violent extremism tends to be heightened. Violations of international human rights law committed in the name of state security can facilitate violent extremism by marginalizing individuals and alienating key constituencies, thus generating community support and sympathy for and complicity in the actions of violent extremists. Violent extremists also actively seek to exploit state repression and other grievances in their fight against the state.”

Some of the contributors of this Handbook have arrived at similar conclusions. The editor argued in chapter 2, when discussing upstream prevention on the national level, that there should be four pillars to build successful preventive anti-terrorist measures on:

- “Good Governance – because, when governance is bad, resistance against corrupt rule gains followers and support and might take the form of terrorism;
- Democracy – because, when unpopular rulers cannot be voted away by democratic procedures, advocates of political violence find a wider audience;
- Rule of Law – because, when rulers stand above the law and use the law as a political instrument against their opponents, the law loses its legitimacy and credibility and encourages people to turn to alternative normative systems;
- Social Justice – because, when long-standing injustices in society are not addressed but allowed to continue for years, without any light in sight at the end of the tunnel, desperate people, and some others championing their cause, are willing to die and to kill for what they perceive to be a just cause.”

Further parallels between the UN Plan of Action and findings by contributors of this volume can also be found when it comes to the importance of involving civil society.

3. Engaging Communities

The UN Plan of Action noted, regarding the importance of engaging communities, in point 51:

“For their survival, violent extremists require the tacit support of a wider circle of sympathizers. If violent extremists can be deprived of this support, their capacity to cause harm and evade justice will be greatly reduced. While
engagement with communities marked by a long history of distrust of the government can pose a challenge, there are a number of community engagement strategies that hold promise. I therefore recommend that Member States: (a) Develop joint and participatory strategies, including with civil society and local communities, to prevent the emergence of violent extremism, protect communities from recruitment and the threat of violent extremism, and support confidence-building measures at the community level by providing appropriate platforms for dialogue and the early identification of grievances.

Again, this is in line with observations made by some contributors of this Handbook. For instance, Rob de Wijk emphasizes the same point in different words:

“Military establishments have learned that insurgency and terrorism are part of a broader political struggle with the populace as center of gravity. Consequently, both COIN and CT doctrine should be population centric. Protecting the population is the key to success in any counterinsurgency campaign. A “hearts and minds” campaign is a prerequisite for gaining the support of the population. This should not be confused with softness. It is an essential activity to prevail in a political struggle. It requires responsible leaders to abstain from harsh rhetoric stigmatization of sectors of society vulnerable to terrorist appeals and refraining to contribute to polarization between majority and minority groups in society. Political leaders ought to respect group identities and grievances, and should take socio-economic measures to take away (some of) the grievances. At the same, they should be aware that jihadists and other militants will try to deprive the population from a sense of security.”

It is common knowledge that youth are especially vulnerable to the lure of terrorism. Yet, young people can also become a crucial actor in preventing and countering terrorism.

4. Empowering Youth:

In his Plan of Action, Ban Ki-moon observed under the heading Empowering Youth (Point No. 52):

“We must pay particular attention to youth. The world’s 1.8 billion young women and men constitute an invaluable partner in our striving to prevent violent extremism. We have to identify better tools with which to support young people as they take up the causes of peace, pluralism and mutual respect. The rapid advance of modern communications technology also means that today’s youth form a global community of an unprecedented kind. This interconnectivity is already being exploited by violent extremists; we need to reclaim this space by helping to amplify the voices of young people already promoting the values of mutual respect and peace to their peers.”

This emphasis on the role of youth is also present in Thomas Samuels’ contribution to this Handbook:

“…the authorities would be missing a golden opportunity should they not realize that not only are educational institutions vulnerable to violent
extremism but ironically, given the right support, they have the potential of becoming citadels for preventing and countering violent extremism among the youth. Simply put, schools and universities can move from being possible breeding grounds for potential sympathizers and recruits to instead actively preventing and countering violent extremism. “….the best defense against extremist ideologies taking over our institutions of learning is to develop an education system that will prepare and equip the students to take on, debate and defeat extremist thoughts where it first takes roots - in the hearts and minds of young people.”19

Regarding the next substantive priority area in the UN Plan of Action, gender equality and empowering women, the Plan of Action has more to say than the Handbook’s contributors.

5. Gender Equality and Empowering Women

The Plan of Action notes in section No. 53 that:

“Women’s empowerment is a critical force for sustainable peace. While women do sometimes play an active role in violent extremist organizations, it is also no coincidence that societies for which gender equality indicators are higher are less vulnerable to violent extremism. We must therefore ask ourselves how we can better promote women’s participation, leadership and empowerment across society, including in governmental, security sector and civil society institutions. In line with Security Council resolution 2242 (2015),20 we must ensure that the protection and empowerment of women is a central consideration of strategies devised to counter terrorism and violent extremism. (…) (c) Include women and other underrepresented groups in national law enforcement and security agencies, including as part of counter-terrorism prevention and response frameworks….”21

Andreas Schädel and Hans-Joachim Giessmann make the same point when they write:

“Research has shown that peace processes are – on average – more sustainable and more effective if they are inclusive and participatory. This applies in particular to the inclusion of representatives of civil society (e.g. religious leaders, women organizations, youth groups), which have been shown to make a successful negotiation and implementation of a peace process more likely.22 Research by Ricigliano (2005), Dudouet (2009) and Toros (2012) has shown that this positive effect is also pertinent for non-state armed groups.23 Expanding inclusion in their direction reduces incentives for the strategic use of spoiler violence during negotiations and has a strong potential to limit post-agreement violence.”24

Parallel findings between the UN Plan of Action and this Handbook can also be found in the sixth issue area addressed in the Secretary-General’s plan.

6. Education, Skill Development and Employment Facilitation

The UN Plan of Action noted in its point 54 on the issue of education, skills development and employment facilitation:
“As part of the struggle against poverty and social marginalization, we need to ensure that every child receives a quality education which equips him or her for life, as stipulated under the right to education. Education should include teaching respect for human rights and diversity, fostering critical thinking, promoting media and digital literacy, and developing the behavioral and socioemotional skills…. (…) (b) Implement education programs that promote “global citizenship,” soft skills, critical thinking and digital literacy, and explore means of introducing civic education into school curricula, textbooks and teaching materials. Build the capacity of teachers and educators to support this agenda….”

Thomas Samuels, in his chapter for this *Handbook*, also stressed the role of education, writing:

“The education sector could conceptualize, develop and impart both mental and emotional ‘firewalls’ into the hearts and minds of the students. In this regard, certain values, skill-sets and awareness such as: (i) Critical thinking; (ii) Empathy; (iii) Diversity; (iv) Resilience; and (v) Awareness on the failures of violent campaigns and the power of non-violent social movements should be developed and institutionalized into the education system. These firewalls could provide a barrier against the radicalization process targeting the students. (…) Institutions of learning such as schools and universities should play an essential role in developing and facilitating a critical mind among their students to enable them to make sound choices and decisions when confronted with the ideology, rhetoric and propaganda of violent extremists. All students should be taught basic cognitive skills such as how to distinguish facts from opinions, identify unstated assumptions and biases in an argument, evaluate the reliability of evidence presented to them….”

7. Strategic Communications, the Internet and Social Media

When it comes to the last of the seven substantive priority areas, strategic communications, the internet and social media, the Plan of Action of the UN notes in section No. 55:

“The manipulative messages of violent extremists on social media have achieved considerable success in luring people, especially young women and men, into their ranks. While violent extremists have demonstrated some sophistication in their use of old and new media tools, it is equally true that we who reject their message have largely failed to communicate to those who are disillusioned and disenfranchised a vision of the future that captures their imagination and offers the prospect of tangible change. Thousands of young activists and artists are fighting back against violent extremism online through music, art, film, comics and humor, and they deserve our support. I therefore recommend that Member States: (a) Develop and implement national communications strategies, in close cooperation with social media companies and the private sector, that are tailored to local contexts, gender sensitive and based on international human rights standards, to challenge the narratives associated with violent extremism…”
In this Handbook, several contributors have addressed the crucial role of media, and in particular the Internet and social media. In chapter three, Sarah Zeiger and Joseph Gyte examined areas of how prevention of radicalization online might be possible:

“1) preventing the spread of terrorist content online (deterring producers), 2) empowering online communities to counter the narratives of violent extremism and terrorism online and promote positive and alternative messages, and 3) building digital resilience and media literacy (reducing the appeal).”

Regarding the third area - building online resilience and literacy – Zeiger and Gyte observe:

“A third and final strategy for the prevention of terrorism online is through building digital resilience and media literacy skills. This is premised on two assumptions: 1) that by building digital resilience and media literacy, the average citizen is able to peacefully overcome grievances that might lead to radicalization that are based incorrectly on misinformation or disinformation; and 2) that a citizen that is able to evaluate both the content of the information provided and the credibility of the source more effectively, would less likely be persuaded by terrorist propaganda. (…) It is important, therefore, that skills and mechanisms for building digital and media literacy are enhanced as part of a comprehensive way of preventing terrorism online and in social media. This means that potentially vulnerable youth should be equipped with the appropriate skills to navigate the challenging communications environment they experience every day, including a large social media presence online.”

In sum, these seven substantive priority areas of the UN Plan of Action are well supported by the evidence assembled by the contributors of this Handbook. There are more similarities between the UN Plan of Action of 2015 and the qualitative findings and suggestions of the contributors of this Handbook. The Appendix to this chapter reprints the entire UN Plan of Action so that the reader can explore these parallels in more detail.

**The UN Plan of Action in the Light of Quantitative Statistical Evidence**

While the overlap between the UN Plan of Action and the qualitative findings of the contributors of this volume are encouraging, it is also worth looking whether these are also supported by more quantitative scientific evidence on terrorism that is based on cross-country and longitudinal comparisons. It is to this we turn next.

The most widely used database on terrorism has been developed at the University of Maryland where its START project maintains a Global Terrorism Database (GTD) listing over 170,000 terrorist incidents since 1970. Based on this and other datasets, the Australian Institute for Economics and Peace (IEP) in Sidney has applied structural equations modelling and correlation analysis using data covering the period 2002-2019. It has done so for countries with advanced economies as well as for developing countries. IEP found that while there is substantial overlap in the strength of association between terrorism and structural indicators, there is also divergence between these two groups of countries.

The researchers at the Institute for Economics and Peace looked at 13 indicators and their relationship with terrorism. The higher the correlations (i.e., closer to 1), the stronger the association between indicators and terrorism.

Based on its statistical data analysis, the Institute for Economics & Peace arrived at findings such as, “Some socio-economic factors associated with terrorism include:
• High levels of group grievance and a weak rule of law is correlated with terrorism across all countries.
• In the more economically developed countries, social disenfranchisement and exclusion play an important role in terrorism.
• In less economically developed countries, religious or ethnic ruptures, and corruption are more strongly associated with high levels of terrorism.”

The more than 70 recommendations contained in the UN Plan of Actions (which profited from the advice of "internal and external experts, scholars and practitioners”29) address many of these relationships between terrorism and IEP indicators. Here are some examples in Figure 1.

**Figure 1. Correlations between Socio-economic Factors and the Global Terrorism Index, 2002–2019 (IEP, 2020)**

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Countries with Advanced Economies</th>
<th>Rest of the World</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Group grievance</td>
<td>0.25</td>
<td>0.67</td>
</tr>
<tr>
<td>2. Factionalized Elites</td>
<td>0.12</td>
<td>0.48</td>
</tr>
<tr>
<td>3. Prosperity</td>
<td>0.04</td>
<td>0.38</td>
</tr>
<tr>
<td>4. Corruption</td>
<td>0.02</td>
<td>0.33</td>
</tr>
<tr>
<td>5. Religious and Ethnic Tension</td>
<td>0.32</td>
<td>0.58</td>
</tr>
<tr>
<td>6. Rule of Law</td>
<td>0.05</td>
<td>0.29</td>
</tr>
<tr>
<td>7. Human Rights Protection</td>
<td>0.42</td>
<td>0.63</td>
</tr>
<tr>
<td>8. Equality and Liberty</td>
<td>0.2</td>
<td>0.63</td>
</tr>
<tr>
<td>9. Military Expenditure</td>
<td>0.17</td>
<td>0.28</td>
</tr>
<tr>
<td>10. Internal Conflict</td>
<td>0.62</td>
<td>0.69</td>
</tr>
<tr>
<td>11. Organized Crime</td>
<td>0.33</td>
<td>0.34</td>
</tr>
<tr>
<td>12. Physical Violence</td>
<td>0.47</td>
<td>0.42</td>
</tr>
<tr>
<td>13. NEET (%)</td>
<td>0.26</td>
<td>0.15</td>
</tr>
</tbody>
</table>

The factor of internal conflict measures politically motivated violence and its impact on governance scored highest, (0.62 for economically advanced countries and 0.69 for the rest of the world in the table above). The researchers of the IEP therefore concluded:

“….that although internal conflict has different characteristics and levels of intensity in countries with advanced and non-advanced economies, the overall impact of this indicator on terrorism is similar in both sets of countries. Over the past two decades, conflict has been one of the strongest predictors of the impact of terrorism, with just under 95 per cent of deaths from terrorism occurring in countries involved in conflict.”

This is also reflected, in point 30 of the UN Plan of Action:

“Prolonged and unresolved conflicts tend to provide fertile ground for violent extremism, not only because of the suffering and lack of governance resulting from the conflict itself but also because such conflicts allow violent extremist groups to exploit deep-rooted grievances in order to garner support and seize territory and resources and control populations. Urgent measures must be taken to resolve protracted conflicts.”
The researchers who wrote the IEP report also looked at the impact of government repression which is represented in the indicator “physical violence” (meaning “violence committed by government agents” in the IEP report\textsuperscript{12}). This factor (0.47 for economically advanced countries, 0.42 for the rest of the world) has also been addressed in the UN Plan of Action’s point 27:

“….Governments that exhibit repressive and heavy-handed security responses in violation of human rights and the rule of law, such as profiling of certain populations, adoption of intrusive surveillance techniques and prolongation of declared states of emergency, tend to generate more violent extremists.”

The factor “issues related to insufficient human rights protection” of the IEP report (scoring 0.47 for economically advanced countries and 0.63 for the rest of the world) is addressed in the UN Plan of Action under points 18, 19, and 20.

“We need to end impunity for all those committing violations and crimes, including crimes under international law. At the same time, we must be vigilant in ensuring that Member States’ efforts to address violent extremism are respectful of the rule of law, and in accordance with their obligations under international human rights law, as well as international humanitarian law…."

It is well known that in many countries there is a nexus between terrorist groups and organized crime groups. The factor “strength of organized crime groups,” identified by the Institute of Economics and Peace (scoring 0.33 for economically advanced countries and 0.34 for the rest of the world), is reflected in the UN Plan of Action under point 14:

“….terrorist groups are also benefiting from transnational organized crime. Some violent extremist groups have developed connections with transnational organized crime to increase their financial resources. They generate significant revenue form human trafficking and the slave trade, trafficking in antiquities, and the illicit sale of oil. Many of these groups are also involved in kidnapping for ransom.”

The issue of “religious and ethnic tensions,” identified by the IEP as a correlating factor (scoring 0.32 for economically advanced countries and 0.58 for the rest of the world) and probable cause is partly addressed in the UN Secretary-General’s Plan of Action under points 28 and 36:

“The lack of adequate efforts, in line with international obligations, towards the realization of economic, social and cultural rights, exacerbated by discrimination against ethnic, national, gender, racial, religious, linguistic and other groups and the absence or curtailment of democratic space, can provide opportunities for exploitation by violent extremists.

Violent extremist groups cynically distort and exploit religious beliefs, ethnic differences and political ideologies to legitimize their actions, establish their claim on territory and recruit followers. Distortion and misuse of religion are utilized to divide nations, cultures and people, undermining our humanity. Faith and community leaders are critical in mentoring vulnerable followers so as to enable them to reject violent ideologies and in providing opportunities for intra- and interfaith dialogue and discussion as a means of promoting tolerance, understanding and reconciliation between communities. Leaders,
Governments, the international community and the media have to work together to prevent confrontation and polarization within and between countries, faiths, nations and peoples.”

The issue in the IEP report, “high share of youth Not in Education, Employment or Training,” abbreviated by IEP as NEET (scoring 0.26 for economically advanced countries and 0.15 for the rest of the world) as a probable cause of terrorism, is partly covered in the UN Plan of Action under the heading “Lack of socioeconomic opportunities” (No. 25):

“Countries that fail to generate high and sustainable levels of growth, to create decent jobs for their youth, to reduce poverty and unemployment, to improve equality, to control corruption and to manage relationships among different communities in line with their human rights obligations, are more prone to violent extremism and tend to witness a greater number of incidents linked to violent extremism. Citizens may consider weak development outcomes as confirmation of the lack of a government’s legitimacy, making state institutions less effective in responding to violent extremism when it arises. The absence of alternative employment opportunities can make violent extremist organizations an attractive source of income.”

The issue of “group grievances” which IEP found to be a probable causal factor in both advanced and developing countries, (scoring 0.25 for economically advanced countries and 0.65 for the rest of the world) can be found in the Plan of Action at various points, e. g. under points 23 and 35:

“Qualitative research, based mainly on interviews, suggests that two main categories of drivers can be distinguished: “push factors,” or the conditions conducive to violent extremism and the structural context from which it emerges; and “pull factors,” or the individual motivations and processes, which play a key role in transforming ideas and grievances into violent extremist action.

Historical legacies of, or collective grievances stemming from, domination, oppression, subjugation or foreign intervention can enable narratives of victimization to take hold. These narratives can provoke simple and powerful emotional reactions which may then be exploited by violent extremists: the memory of past or present actual or perceived oppressions is upheld so as to fuel the thirst for revenge against oppressors.”

The issue of “lack of prosperity” (scoring 0.04 for economically advanced countries and 0.38 for the rest of the world) has been addressed in the Plan of Action under point 25 (“Lack of socioeconomic opportunities”) mentioned above.

In sum, it can be concluded that the observations, findings and recommendations of the UN Plan of Action have a solid empirical basis since its main points are not only supported by the findings of the expert contributors to this Handbook but also by the statistical evidence gathered by the Institute of Economics and Peace. Given the soundness of the UN Plan of Action, one would expect that the international community would make good use of this solid plan and member states would immediately recalibrate their national responses to terrorism in its light. However, the UN Plan of Action has, in the last six years, not made as much progress as one could have hoped for. There are several reasons for this.
The Reception of the UN Plan of Action by UN Member States

The UN Secretary-General, in his Plan of Action from late 2015, left the definition of “violent extremism” to national authorities, although he cautioned that national definitions must be consistent with international law and international human rights law. The UN’s Global Counter-Terrorism Strategy of September 2006 had already avoided defining “terrorism” since the discussion of a Comprehensive Convention on International Terrorism in the Ad Hoc Committee of the 6th (legal), Committee of the General Assembly, initiated in 2000, had not produced a consensus on this issue by 2006 (or for that matter: by 2021).

Later, the UN also did not manage to arrive at a common definition of “violent extremism.” Therefore, both terms - “terrorism” and “violent extremism” - can be interpreted by each UN member state more or less as convenient for itself. Just how divergent UN member states interpret (violent) extremism, emerged from an analysis of the UN Office of the High Commissioner for Human Rights from October 2016:

“Some domestic laws and policies address the phenomenon of ‘extremism’ without qualifying it as ‘violent’. They define ‘extremism’ as ‘vocal or active opposition’ to the values of the respective country or society, including ‘democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs’.

Some definitions of ‘extremism’ refer to notions or aims which are racist, anarchist, nationalist, authoritarian or totalitarian regardless of their political, ideological, religious or philosophical character, and which are contrary, in theory or in practice, to principles of democracy or human rights, to the good functioning of the democratic institutions of the State or to other basic principles of the rule of law. Some laws and policies go further and describe extremism as encompassing non-violent conduct, including conduct deemed to insult national pride or breach national dignity, or knowingly disseminating false accusations against federal or regional officials, such as allegations that they have committed illegal or criminal act in their official capacity. If they are not limited to ‘violent’ extremism, such measures risk targeting the holding of an opinion or belief rather than actual conduct.”

Another problem which the Plan of Action to Prevent Violent Extremism of 2015 shares with the Global Counter-Terrorism Strategy of 2006 is its non-binding character. In the new Plan of Action UN member states were only invited to “… consider the implementation of relevant recommendations of the Plan of Action, as applicable to the national context.” Since the UN is an international and not a supra-national organization, it can only “…support Member States and regional organizations at their request and only with their consent.”

This is a major obstacle to creating a seamless and effective international regime against terrorism. Some UN resolutions, such as UN Security Council 1373 of 28 September 2001, were passed under chapter VII of the UN Charter and, therefore, became binding for all member states. They require member states to periodically report on their national implementation. No such monitoring mechanism exists for the Plan of Action - a Plan of Action which was not formally adopted by the General Assembly but only ”welcomed” and “taken note of.”

The Plan of Action was presented to the General Assembly at a time when IS (Daesh) was at the height of its power by the outgoing UN Secretary-General Ban Ki-moon, who earlier that year had been prodded by US President Obama. However, the Plan of Actions reception in the General Assembly was muted: The national representatives first merely “noted” its existence and later, during a periodical review of the Global Counter-Terrorism Strategy of 2006, member states were merely invited to “consider” the Plan of Action ”in accordance with their priorities.”

When the UN promotion of the Plan of Action passed into the hands of a senior Russian diplomat, V.I. Voronkov, it ended up at the end of his list of priorities.
The traditional Russian approach to terrorism has generally been characterized by a preference for repression rather than prevention—an approach shared by China, like Russia a permanent member of the Security Council with veto power. Resistance to the Plan of Action came from other sides as well (e.g., Egypt). As David Ucko explained, there was

“….a perception of some member-states that the Secretary-General had forced PVE through without adequate capturing their concerns. The Global South tends to seen the UN as dominated by the West … and its work with counter-terrorism as answering to a distinct American call. (…) At Turtle Bay [area of the UN headquarters in New York], governments and NGOs alike greeted PVE with caution and became reliant, once more, on old talking points. PVE’s thinly concealed American provenance, alongside the unchanged structural inequities of the UN, produced legitimacy problems, particularly for those who felt most slighted by the UN’s earlier work on counter-terrorism, specifically Muslim-majority countries. Others, like Russia and China, resisted the PVE’s elevation of civil society and human rights and worked hard to limit the effect of such language. (…) In June 2018, during a period review of the UN Global Strategy of 2006, some UN member states tried (but failed) to erase mentioning the Plan of Action. However, they managed to ensure that the resolution did not include a full endorsement of the Plan of Action which some other UN member states sought.” 42

The lack of enthusiasm for a preventive approach to terrorism involving the “whole-of-society” (read, civil society in many countries) reflects a global shift of governance away from democracy, accompanied with higher levels of repression of even peaceful dissent. 43

While democracy first spread on all continents after the end of the Cold War, it has receded considerably since the beginning of the 21st century when there were 120 democracies in the world. By 2019, more than one third of humankind lived under authoritarian rule. Among 167 major states monitored by The Economist’s Intelligence Unit, there were, by 2019, only 22 “full democracies” and their population amounted to only 5.7 percent of the world’s population. The rest of humankind have to live in “flawed democracies” (54 countries with 42.7 percent of the world population); or under “hybrid regimes” (37 countries with 16 percent of the world population) or, even worse, under “authoritarian regimes” (54 countries with 35.6 percent of the world population) according to The Economist’s report on the world’s “Status of Freedom and Democracy.” The downwards trend continued since 2019: democratic freedoms became less in 116 out of 167 countries in 2020 (Economist Intelligence Unit).44

The decline of democracy matters when it comes to levels of terrorism. While free and open societies are more vulnerable to terrorism, they also tend to produce less (domestic) terrorism due to the greater responsiveness of democratic governments to the will of the (majority of the) people and the government’s adherence to the rule of law.45 This is also confirmed by the IEP report, which concluded, on the basis of statistical analysis:

“The prevalence of violence will be greater where groups feel unable to seek peaceful resolution and remediation because the political or judicial systems are perceived as ineffective or biased. (…) Deficient protection of human rights is associated with terrorism in nations of all stages of development. (…) Deficient rule of law and equality before the law can promote terrorist activity among developing nations. This is because marginalized groups cannot address their grievances and demands through the courts or political systems in a peaceful manner.”46
In the case of the UN Plan of Action, active or passive resistance came mainly from non-democratic member states, in particular Muslim-majority countries. The outgoing Secretary-General Ban Ki-Moon was a “lame duck” as his term was about to expire. In the negotiations for his succession, Russia demanded and got (among other concessions) the chief mandate for counter-terrorism in return for not objecting to António Guterres becoming Secretary-General. At the same time, the new American President, Donald Trump, was no believer in his predecessor’s proposed alternative to the War on Terror, which under President Obama, went under the caption “Countering Violent Extremism” (CVE).\textsuperscript{47} While President Trump allowed the State Department to switch terminology from CVE to Prevention of Violent Extremism (PVE), few new resources and initiatives resulted from this change.\textsuperscript{48} Until 2021, UN Secretary-General Guterres lacked the backing of the US government in pushing the Plan of Action further; putting a Russian diplomat in charge of the Plan of Action was not considered particularly helpful to its implementation.

While various UN agencies have been tasked to take initiatives for the promotion of the Plan of Action, it is ultimately the duty of member states and, secondarily, regional organizations, to take the necessary steps. A brief look at this does not give much cause for optimism.

**Regional and National Plans of Actions**

Various regional organizations have, in the wake of the UN Plan of Action, formulated their own prevention-oriented plans, or adapted and updated existing ones. Among these are the Organization for Security and Co-operation in Europe (OSCE),\textsuperscript{49} the European Council,\textsuperscript{50} and the European Union.\textsuperscript{51}

For instance, the Council of Europe (which has 47 member states, 27 from the European Union, and includes Russia), launched a Counter-Terrorism Strategy (2018-2022). It highlights, next to emphasizing the role of prosecution and protection, also prevention. In the Annex to this strategy document, the Council of Europe proposed prevention activities such as a “…compilation of best practices on how to prevent and counter terrorist public provocation, propaganda, radicalization, recruitment and training on the internet, while respecting human rights and fundamental freedoms, the rule of law and democracy.” It also proposed “…establishing a set of risk indicators for identifying individuals likely to become “terrorists acting alone.”\textsuperscript{52}

The European Union developed a new prevention-orientated program in December 2020, following a series of terrorist attacks in major European cities, including one in Vienna, titled “A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond.” Its two prevent elements were described in these terms:

“Firstly, we need to be able to better anticipate existing and emerging threats in Europe. Information sharing and a culture of cooperation that is multidisciplinary and multi-level remain key for a solid threat assessment that can form the basis of a future-proof counter-terrorism policy.

Second, we need to work to prevent attacks from occurring, by addressing and better countering radicalization and extremist ideologies before they take root, making clear that respect for the European way of life, its democratic values and all it represents is not optional. This Agenda sets out ways of supporting local actors and building more resilient communities as a matter of priority, in close coordination with Member States, taking into account that some attacks have also been carried out by Europeans, raised within our societies, who were radicalized without ever having visited a conflict zone.”\textsuperscript{53}
The European Commission proposed “…setting up an EU Knowledge Hub on the prevention of radicalization and support[ing] national networks of stakeholders and national centers” as well as “…Build community resilience through the measures included in the Action Plan on integration and inclusion.”

Since 2016, a substantial number of UN member states have elaborated national Plans of Action, generally assisted by UN entities like UNDP, and UNOCT. Various think tanks also developed helpful suggestions on how to turn the UN Plan of Action into a national reality. One such plan was developed by the Washington-based Global Center on Cooperative Security. It consists of six steps:

1. **Establish**: Countries should systematically identify stakeholders to ensure that a wide range of interest groups are considered in shaping, informing, and legitimizing the development and adoption of a national strategy. Countries should work to sustain the involvement of multi sector stakeholders at all stages of the strategy development process, incorporating perspectives, experiences, and recommendations in the prioritization of policy measures.

2. **Gather**: Countries should ensure that a baseline of relevant research is assessed prior to strategic adoption. This baseline must be sufficient to justify the need for the strategy and the relevance of its policy measures and to identify knowledge gaps to target future research activities.

3. **Analyze**: Countries should define the problems that the strategy seeks to address, distinguishing among key terms and describing their conceptual relationships. Definitions should be locally relevant, used consistently, and developed in line with international law. Countries should describe the national drivers of violent extremism, explicitly referencing the available evidence and its relationship to the problems the strategy aims to address.

4. **Develop**: When evidence about problems identified at a national level is limited, the policy measures developed should be modest, prioritizing research on the problems and their causes to better inform the identification of future policy measures. Countries should present the objectives of policy measures and outline these measures are intended to contribute to strategy outcomes. When policymakers propose targeted policies to reduce support for violent extremist groups, causes, or ideologies, these policies should be connected to specific domestic drivers and a target group.

5. **Implement**: Countries should identify the role of different stakeholders in the implementation of policy measures, describing their working relationships and the mechanisms established to share information and coordinate strategy implementation. Countries should include an implementation road map that includes milestones and dates for completion of specific policy measures and resources secured or required to implement each measure successfully.

6. **Monitor**: Countries should identify mechanisms for monitoring strategy implementation and impact, including when evaluation will take place, who will conduct it, how and where the evaluation will be made available, and how the road map will contribute to future strategy revisions. Countries should ensure that their strategies are the product of an evidence-based process that sets out the proportionality of identified interventions, establishing monitoring and evaluation mechanisms that are sensitive to the impact of the strategy on human rights and fundamental freedoms of citizens.

The UN, in its Reference Guide on Developing National and Regional Action Plans to Prevent Violent Extremism, recognized that “A one-size-fits-all model for a PVE plan does not
exist.” For this as well as other reasons, regional organizations and member states felt encouraged to find their own solutions.

It would go beyond the scope of this chapter to analyze all regional and national plans of actions that emerged since 2016. Unfortunately, in many cases, these national plans of action remained little more than paper exercises since many governments lack either the political will or the economic resources (or both) to effectively implement them. An example of this can be found in Lebanon. The author of a case study on this country noted:

“The real efforts from the Lebanese government to quickly implement the United Nations Plan of Action on Preventing Violent Extremism should be acknowledged, encouraged and supported. Indeed, Lebanon can be seen as a pioneer amongst other countries in the Middle East for its swift welcoming of this initiative, and its readiness to develop a national strategy. This said, a close analysis of the Lebanese Strategy reveals major shortcomings which might affect its internal coherence. Lebanon’s lack of the necessary means or capacity only years of development can provide will encumber the effective implementation of the policies introduced in the strategy. More importantly, no significant reforms, necessary to the effective implementation of the Strategy will happen without a profound break from the political paradigm that emerged in the aftermath of the civil war, marked by sectarianism, feudalism, clientelism, nepotism and corruption on every decision made at every level of government. (…) Without abandoning the very system that has been the root cause of people’s mistrust in the state including poor governance, sectarianism and corruption among other grievances, the government will fail to tackle the drivers of violent extremism conducive to terrorism in the country. Beyond the empty words of its PVE Strategy, the Government’s inaction to address the legitimate grievances of the people … have clearly shown that the political apparatus has no real desire to make such a drastic change.”

Rather than further elaborating on the incomplete implementation of the UN Plan of Action, this final chapter of the Handbook will be concluded with some reflections on strategy.

**From Plans of Action to an Action Strategy**

The UN Plan of Action is a plan, not a strategy. Lawrence Friedmann explained the difference: “A plan supposes a sequence of events that allows one to move with confidence from one state of affairs to another. Strategy is required when others might frustrate one’s plans because they have different and possibly opposing interests and concerns.” In this narrow sense, the UN Plan of Action is not even a plan as it lacks the element of sequencing and sufficient commitment from UN member states. It is certainly not a strategy - but then, again, the definition issue arises.

What is strategy? Like with many other key concepts in the field of security studies, there is no single, commonly accepted, definition. The short classic 19th century definition of Carl von Clausewitz, describing strategy as “… the doctrine of the use of individual battles for the purposes of war” will no longer do. The 21st century thinker who has explored the concept of strategy most thoroughly for our times is Lawrence Freedman. The following definition of strategy, developed by the editor of this volume, is indebted to Lawrence Freedman, Gregory Miller, as well as Tore Bjørgo, but goes beyond their definitions. Strategy refers, usually in a situation of competition or conflict:
1. To a flexible plan to determine and pursue, for the short-, medium- or long term, the best possible course of action, given the prevailing constraints and foreseeable circumstances, to advance desirable, but realistic objectives.

2. This can be achieved by judicious and creative utilization of available resources - including the mobilization of human, spiritual (cultural or religious narrative themes) and material (natural, financial and technical) resources - as well as

3. The building of coalitions with third parties who have similar interests or objectives.

4. With the combined application of political, diplomatic, military, economic, intellectual (Research & Development) and media (incl. cyber & propaganda) instruments – and

5. Based on sufficient insight into the adversary’s current and evolving interests, objectives and strategy (including its strengths and weaknesses).

As a consequence of the more skillful utilization of these five elements than the opponent, the relative power distribution between “us” and “them” can be expected to be shifting to one’s own advantage, leading to strategic success.68

What are some of the implications of this conceptualization of strategy when it comes to developing strategies of terrorism prevention? Here are some, admittedly rudimentary, reflections on each of these five points as these relate to the prevention of terrorism.

Regarding the first point: To a flexible plan to determine and pursue, for the short-, medium- or long term, the best possible course of action, given the prevailing constraints and foreseeable circumstances, to advance desirable but realistic objectives. The objectives not only need to be desirable but also realistic. To “… completely eradicate radical Islamic terrorism from the face of the earth,” as US president Donald Trump announced when he took office on 20 January 2017 was not realistic.69 If the tool to engage in an act of terrorism is as widely available as a truck that can be driven into a crowd by a single person, it is not realistic to expect this to end. Nor is it realistic to assume that the mass and social media will not report it and thereby create feelings of terror beyond the immediate witnesses to the crime. The ubiquity of tools and the wide presence of (social) media are “prevailing constraints” under present circumstances. Making “flexible plans” is possible, based on various scenarios (e.g., for “high impact but low probability attacks,” and for “low impact but high probability attacks”). What is important is not only to make short-, medium and long-term plans but also to pursue these through training, involving, inter alia, “Red Teaming,” that is, testing existing defenses with the help of an attack team playing the role of terrorists in a realistic scenario. The UN Plan of Action was also stressing the “flexible” nature of plans by writing,

“….our actions have to be as agile and far-reaching as the phenomenon itself. We have to improve our set of tools dynamically and keep reviewing our responses. The Plan of Action constitutes the inaugural basis for a comprehensive approach to this fast evolving, multidimensional challenge.”70

When it comes to “foreseeable circumstances” in the definition of strategy, this means constructing various scenarios with different potential future outcomes and engage in role-playing to explore each of these more or less likely “foreseeable circumstances.”

Regarding the second point: the judicious and creative utilization of available resources, including the mobilization of human, spiritual (cultural, religious, normative narrative themes) and material (natural, financial and technical) resources. The availability of resources varies from actor to actor. The terrorist needs only a few: he (or she) has the element of surprise on his/her side and might, with a weapon be dominant at a place and time of his (or her) own choosing for just a few minutes, counting mainly on the media-based reverberations of the terrorist act in and beyond the community where the attack takes place. The government’s side has vastly more resources but these are generally not available in time for prevention without
advance intelligence (human or signal) about the where, when and from whom to expect what kind of attack. If the government is democratically elected and society is not too polarized, it can speak from the moral high ground and thereby has a normative advantage over those who commit what would be “war crimes” in war. This moral high ground is an enormous resource if properly utilized. A sizeable part of terrorism is, however, the result of governments acting unjustly and thereby forfeiting the normative advantage.

One of the best ways for governments to prevent (some if not all) terrorism is to stick to the rule of law and to treaty-based human rights and humanitarian law obligations. For all we know there will, as a consequence, be less (domestic) terrorism. Since terrorism relies on communication, governments have many technical and legal instruments to control communication channels in combination with mass media editors and technological service providers on the internet. However, such control not only reduces the effectiveness of terrorism as a communication strategy but also tends to reduce ordinary people’s right to express themselves and their right to know. Terrorists admit that more than half of their struggle is in the media but when it comes to preventing terrorism, few resources are devoted to this area, except for the creation and distribution of “counter-narratives” which tend to be of very limited effectiveness as long as words and deeds of governments do not match. Attempts to take down terrorist messages from social media, while increasing, are post-hoc in character and limited to a few languages only. Since terrorism is violence as, and for, communication, more resources ought to be devoted to neutralize terrorist communication efforts. This can only be done in cooperation with owners and editors of mass media and service providers of social media.

Regarding the third point: the building of coalitions with third parties who have similar interests or objectives. Pooling resources and capabilities with others, is the most direct way in what Lawrence Freedman calls “the art of creating power.” The temptation here is to seek also “ unholy alliances” with partners who interests might be temporarily similar but whose ultimate objectives might create problems further down the timeline. Seeking cooperation with only nominally non-violent extremists (like the Muslim Brotherhood) to fight violent extremists (like Al Qaeda), as has occurred in some Western countries after 9/11, is a case in point. A more positive example of coalition-building is how the international resistance against ISIS in Syria and Iraq brought together in 2014 a coalition of 59 states plus the European Union. Yet this point about coalition building applies not only to international coalitions. On the domestic front, government, civil society, business and other stakeholders, including from minority communities and diasporas have to get together and confront terrorism collectively.

Regarding the fourth point: the combined application of political, diplomatic, military, economic, intellectual (Research & Development) and media (incl. cyber & propaganda) instruments. This point roughly coincides with the idea of whole-of-government and whole-of-society approaches. Such a broad securitization of counter-terrorism will, like the coalition building of point 3, augment existing strengths. However, such a combination might not only create the specter of a national security state but might also direct attention away from other, and in some cases, more serious problem areas where government and societal action is sorely needed (such as the threat from organized crime, fighting pandemics, reversing climate change). In the cyber sphere where control is weak, governments have yet to learn how to optimize (and regain) control of hardware infrastructures and software programs to be on the winning side.

Regarding the fifth point: obtaining sufficient insight into the adversary’s current and evolving interests, objectives and strategy (including its strengths and weaknesses). A strategy that does not have a good idea about the opponent’s strategy is generally doomed to failure. So far, this has been one of the weakest elements in efforts to prevent non-state terrorism. It is also almost absent in the UN Plan of Action. There, the only general reference to terrorists’ strategy is the following passage: “Analyses of local and national drivers of violent extremism form and important point of departure for developing national plans.” This is followed by the
recommendation of “Establishing early warning centers for the exchange of information on violent extremist activities….,” The earlier UN Global Counter-Terrorism Strategy, unanimously approved by the General Assembly on 8 September 2006 is, despite its name, also only a plan of action, not a strategy in the sense of our definition of strategy and it is also almost totally silent about the strategy of the terrorist side. The most important thing to remember when it comes to terrorist strategy from non-state actors is that the success of terrorists largely depends on the indirect effects caused by the reactions of governments, media, society and other parties to terrorist provocations and acts of revenge. Yet, these reactions by government and society can, to a considerable extent, be controlled and modified.

There are at several ways in which this last insight can contribute to the prevention of terrorism. Here, to conclude, we only highlight four of these which are also lessons that the attentive reader of this Handbook will already have learned:

1. **Lesson Learned I**: One important cause of non-state terrorism is a desire to exact revenge for some perceived or real injustice that has not been adequately addressed by the existing political system. is a greatly underestimated cause of terrorism. If government actions are within the rule of law, respecting basic human rights and supported by the majority of citizens, there will be fewer people driven to terrorist acts by feelings of revenge. In other words, many acts of retaliatory terrorism by non-state actors will be prevented by avoiding acts of revenge (as opposed to rule of law-based law enforcement).

2. **Lesson Learned II**: Another way of reducing non-state terrorism relates to those acts of terrorism which are acts of provocation. Many terrorists want to produce an over-reaction with their atrocities, expecting that the government will target and repress the terrorists’ professed constituency as a whole, which is likely to drive new recruits into the arms of the terrorist organization. Governments should avoid falling into the trap of doing what terrorists expect. By not falling into the provocation trap, governments can prevent some further acts of terrorism.

3. **Lesson Learned III**: A third way to prevent terrorism is to limit the possibilities for terrorists to obtaining free publicity with their public outrages. If half or more of the terrorist struggle is in the media, prevention should shift more strongly to targeting the communication channels and the mass and social media terrorists seeks to instrumentalize to reach various audiences. Without publicity for their cause, terrorists cannot hope to get very far. However, to reduce the amount of publicity for acts of terrorism, governments have to work closely with editors of mass media and operators of social media and mobilize public support for applying selective news blackouts. This too, will prevent some acts of terrorism.

4. **Lesson Learned IV**: A fourth way of reducing terrorism is based on the fact that terrorism is intimately linked to armed conflict. Becoming a party to an armed conflict abroad might not always be avoidable for governments but should only be done as a last resort in cases of humanitarian emergencies and then only with a strong mandate from the United Nations. Resistance against foreign interventions allows local terrorists to gain support and leads to radicalization among sectors of the public abroad. Terrorism is intimately linked to conflict not only abroad but also on the domestic front. Preventing polarization in society, protecting minorities against hate crimes while engaging in strengthening social cohesion and resilience and engaging in conflict resolution goes a long way in preventing terrorism at home.

These are four clear lessons that have emerged from empirical research on terrorism. Why do many governments not (fully) apply them? It has often been said that there is no glory in prevention. Spectacular counter-terrorist operations, like the assassination of a terrorist leader...
or the dramatic rescue of hostages are portrayed as “successes.” Prevention is largely silent; its success is a non-event - but one arising from foresight and preparedness rather than inaction or reaction only. While much of military counter-terrorism has serious negative repercussions, prevention policies, sensitively applied, are unlikely to do harm as there is no significant collateral damage while significant ancillary societal benefits can result from prevention policies which go far beyond counter-terrorism. Preventive measures are not cheap but they are nowhere as expensive as the Global War on Terror. The outcome of effective prevention is greater security. Yet to become effective, we have to get better at foresight and at identifying possible intervention points – upstream, midstream and downstream – for taking appropriate preventive measures.

The contributors to this volume have offered many thoughtful suggestions about what could and should be done as has the solid, but under-valued UN Plan of Action. As this volume makes clear, solid knowledge about prevention of terrorism exists but implementation of adequate preventive measures still has to wait for political will which, unfortunately, is still in short supply in many places.78

Alex P. Schmid is a Research Fellow at the International Centre for Counter-Terrorism (ICCT) in the Hague, the Netherlands. He is Editor-in-Chief of Perspectives on Terrorism and former Co-Editor of Terrorism and Political Violence – both leading journals in the field of Terrorism Studies. Until 2009, Prof. em. Schmid held a chair in International Relations at the University of St. Andrews where he was also Director of the Centre for the Study of Terrorism and Political Violence (CSTPV). Previous positions include Officer-in-Charge of the Terrorism Prevention Branch of the UN Office on Drugs and Crime in Vienna and a chair in Conflict Resolution at the Erasmus University Rotterdam. Between 1978 and 2018 he also held various positions at Leiden University. Currently, he is Director of the Vienna-based Terrorism Research Initiative (TRI), a consortium of 16 institutes and more than 100 individual scholars seeking to enhance human security through collaborative research. Alex Schmid has more than 200 publication and reports in ten languages to his name, including the award-winning volume “Political Terrorism” (1984, 1988, 2006) and the “Routledge Handbook of Terrorism Research” (2011, 2013).
I. Introduction

1. Violent extremism is an affront to the purposes and principles of the United Nations. It undermines peace and security, human rights and sustainable development. No country or region is immune from its impacts.

2. The present Plan of Action to Prevent Violent Extremism considers and addresses violent extremism as, and when, conducive to terrorism. Violent extremism is a diverse phenomenon, without clear definition. It is neither new nor exclusive to any region, nationality or system of belief. Nevertheless, in recent years, terrorist groups such as Islamic State in Iraq and the Levant (ISIL), Al-Qaida and Boko Haram have shaped our image of violent extremism and the debate on how to address this threat. These groups’ message of intolerance — religious, cultural, social — has had drastic consequences for many regions of the world. Holding territory and using social media for the global and real-time communication of their ideas and exploits, they seek to challenge our shared values of peace, justice and human dignity. The spread of violent extremism has further aggravated an already unprecedented humanitarian crisis which surpasses the boundaries of any one region. Millions of people have fled the territory controlled by terrorist and violent extremist groups. Migratory flows have increased both away from and towards the conflict zones, involving those seeking safety and those lured into the conflict as foreign terrorist fighters, further destabilizing the regions concerned. While the Plan of Action has been developed within this context, it is intended to address violent extremism in all its forms and wherever it occurs.

3. Nothing can justify violent extremism but we must also acknowledge that it does not arise in a vacuum. Narratives of grievance, actual or perceived injustice, promised empowerment and sweeping change become attractive where human rights are being violated, good governance is being ignored and aspirations are being crushed. Violent extremists have been able to recruit over 30,000 foreign terrorist fighters from over 100 Member States to travel to the Syrian Arab Republic and Iraq, as well as to Afghanistan, Libya and Yemen. Some of them will no doubt be horrified by what they see and anxious to put the experience behind them, but others have already returned to their home countries — and more will undoubtedly follow — to spread hatred, intolerance and violence in their own communities.

4. Over the past two decades, the international community has sought to address violent extremism primarily within the context of security-based counter-terrorism measures adopted in response to the threat posed by Al-Qaida and its affiliated groups. However, with the emergence of a new generation of groups, there is a growing international consensus that such counter-terrorism measures have not been sufficient to prevent the spread of violent extremism. Violent extremism encompasses a wider category of manifestations and there is a risk that a conflation of the two terms may lead to the justification of an overly broad application of counter-terrorism measures, including against forms of conduct that should not qualify as terrorist acts.

5. In its resolution 2178 (2014), the Security Council makes explicit the link between violent extremism and terrorism, underscores the importance of measures being in line with international norms and recognizes the need for prevention: “violent extremism, which can be conducive to terrorism,” requires collective efforts, “including preventing radicalization, recruitment and mobilization of individuals into terrorist groups and becoming foreign terrorist fighters.” In that resolution, the Council “calls upon Member States to enhance efforts to counter this kind of violent extremism,” recognizing that “international cooperation and any measures taken by Member States to prevent and combat terrorism must comply fully with the Charter of the United Nations.” Definitions of “terrorism” and “violent extremism” are the prerogative of Member States and must be consistent with their obligations under international
law, in particular international human rights law. Just as the General Assembly has taken a practical approach to counter-terrorism through the adoption by consensus of the United Nations Global Counter-Terrorism Strategy, this Plan of Action pursues a practical approach to preventing violent extremism, without venturing to address questions of definition.

6. There is a need to take a more comprehensive approach which encompasses not only ongoing, essential security-based counter-terrorism measures, but also systematic preventive measures which directly address the drivers of violent extremism that have given rise to the emergence of these new and more virulent groups. In the Charter of the United Nations, Member States resolved to “take effective collective measures for the prevention and removal of threats to the peace.” I have made it a priority to re-energize the Organization’s prevention agenda, especially with respect to preventing armed conflict, atrocities, disasters, violence against women and children, and conflict-related sexual violence, and have launched a dedicated initiative to place human rights upfront. The 2015 report of the High-level Independent Panel on United Nations Peace Operations (see A/70/95-S/2015/446), the report of the Advisory Group of Experts on the review of the United Nations peacebuilding architecture (see A/69/968-S/2015/490), the 2030 Agenda for Sustainable Development [General Assembly resolution 70/1] and the women, peace and security agenda have all stressed the need to build a collective commitment to making prevention work. The spread of violent extremism makes preventive efforts all the more relevant.

7. The United Nations Global Counter-Terrorism Strategy, adopted unanimously by the General Assembly by its resolution 60/288, explicitly addresses prevention and foresees balanced implementation across all four of its pillars: (a) tackling conditions conducive to terrorism; (b) preventing and combating terrorism; (c) building countries’ capacity to combat terrorism and to strengthen the role of the United Nations system in that regard; and (d) ensuring respect for human rights for all and the rule of law while countering terrorism. Over the last decade, there has been a strong emphasis on the implementation of measures under pillar II of the Global Strategy, while pillars I and IV have often been overlooked. Ahead of the tenth anniversary of the adoption of the Strategy, in 2016, I am launching this Plan of Action, with a focus on preventive measures for addressing violent extremism, including by reinvigorating those measures covered under pillars I and IV of the Strategy, ensuring a more comprehensive implementation of the Strategy in view of the lessons learned over the past decade and the challenges that may lie ahead. In the context of its most recent review of the Strategy, the Assembly urged Member States “to unite against violent extremism in all its forms and manifestations.” In doing so, we must be principled and strategic and must calibrate our response carefully. We must refocus our priorities, strengthen our application of justice, and rebuild the social compact between the governing and governed. We need to pay attention to why individuals are attracted to violent extremist groups. I am convinced that the creation of open, equitable, inclusive and pluralist societies, based on the full respect of human rights and with economic opportunities for all, represents the most tangible and meaningful alternative to violent extremism and the most promising strategy for rendering it unattractive.

8. While our understanding of the drivers of violent extremism has improved, enabling us to adapt and refine our actions, we have to accelerate our learning process to counter the speed with which this threat is evolving. While, collectively, we have the tools with which to address many of the grievances driving violent extremism, we have to learn to use and resource them effectively. United Nations entities, including the Counter-Terrorism Implementation Task Force and the United Nations Counter-Terrorism Centre, the Counter-Terrorism Committee Executive Directorate, the United Nations Development Programme, the Office of the United Nations High Commissioner for Human Rights, the United Nations Educational, Scientific and Cultural Organization, the United Nations Office on Drugs and Crime, the United Nations Alliance of Civilizations, the Department of Peacekeeping Operations of the Secretariat, the Peacebuilding Support Office and the United Nations Entity for Gender Equality and the
Empowerment of Women (UN-Women), and my Envoy on Youth, as well as many other members of the United Nations family, have been working on issues relevant to preventing violent extremism. We need to build on lessons already learned to refine our actions and render them more effective.

9. We will not be successful unless we can harness the idealism, creativity and energy of young people and others who feel disenfranchised. Young people, who constitute the majority of the population of an increasing number of countries today, must be viewed as an asset and must be empowered to make a constructive contribution to the political and economic development of their societies and nations. They represent an untapped resource. We must offer them a positive vision of their future together with a genuine chance to realize their aspirations and potential.

10. In developing this Plan of Action, I have listened closely to the views of Member States and regional organizations. We also consulted internal and external experts, scholars and practitioners. I welcome the multilateral initiatives that have stressed the need for creative and innovative action to address violent extremism.

11. The founders of the United Nations believed in the power of our shared principles, purposes and values. Member States are obliged to adapt their actions to new realities without reneging on our common commitments. The moment we consider these common commitments dispensable we help those who disrespect them to achieve their goals. With this Plan of Action, I intend to stimulate global debate on how we can best leverage our comparative advantages to effectively prevent violent extremism.

II. Impact of violent extremism

12. Violent extremism undermines our collective efforts towards maintaining peace and security, fostering sustainable development, protecting human rights, promoting the rule of law and taking humanitarian action.

A. Peace and security

13. Violent extremist groups are contributing significantly to the cycle of insecurity and armed conflict affecting many regions of the world. Al-Qaeda and its affiliates have sought to intimidate Governments into changing their policies through virulent propaganda campaigns and by staging spectacular attacks. The latest iteration of violent extremist and terrorist groups, ISIL in particular, has transformed the challenge further: benefiting from existing armed conflicts in the Syrian Arab Republic and instability in Iraq and in Libya, its members have managed to take over large swaths of territory and “govern” it according to their rules. They are mobile, well-armed, tech-savvy and well organized. History has shown that volatile security situations and conflicts tend to be further exacerbated by “proxy” wars. Regional and international actors bear a particular responsibility for assisting countries in strife in returning to peace. I therefore welcome the recent constructive initiatives taken in the context of the International Syria Support Group, working in concert with the Security Council to promote a comprehensive solution to the crisis in the Syrian Arab Republic.

14. In seeking to supplant existing States and erase established borders, ISIL and Boko Haram are undermining state authority and destabilizing not just the territories most directly concerned, but also the surrounding regions. In Mali, terrorists came close to destroying the basic state structure, thereby affecting the stability of a country and of an entire region. Al-Qaeda in the Islamic Maghreb and other groups continue their activities in northern Mali with spillover effects in neighboring countries. They put the presence and activities of the United

...
Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA) at risk. As I noted in a recent report (S/2015/366), terrorist groups are also benefiting from transnational organized crime. Some violent extremist groups have developed connections with transnational organized crime to increase their financial resources. They generate significant revenues from human trafficking and the slave trade, trafficking in antiquities, and the illicit sale of oil. Many of these groups are also involved in kidnapping for ransom.

15. It is critical that in responding to this threat, we recognize that violent extremists aim at provoking States into overreacting, and then exploit ill-conceived government action for their own propaganda ends. In killing 77 people in 2011, the Norwegian mass murderer Anders Breivik was explicitly aiming at destabilizing Norway’s tolerant society by dividing local communities and provoking an overreaction. The obligations that Member States have undertaken in line with international law, including human rights instruments, provide a sound framework within which to respond to such attacks.

B. Sustainable development

16. Countries struggling to cope with widespread violence have fared poorly in reaching the Millennium Development Goals which have shaped the development agenda over the last 15 years. Violent extremism aggravates perceptions of insecurity and can lead to repeated outbreaks of unrest which compromise sustained economic growth. In establishing the Sustainable Development Goals to guide our work over the next 15 years, Member States warned that violent extremism threatens to reverse much of the development progress made in recent decades. By exploiting development challenges, such as inequalities, poverty and poor governance, violent extremism further exacerbates these grievances and thereby creates a vicious cycle of decline which affects marginalized groups in particular. Moreover, considering education a particular threat to the spread of their ideologies, terrorists have targeted young people, in particular girls, for their pursuit of modern education as the path to a better life for themselves and their families and better societies. The kidnapping of girls by Boko Haram in Chibok, Nigeria, in April 2014; the killing of students by Al-Shabaab in Garissa, Kenya, in April 2015; and the attack by Tehrik-i-Taliban on the Army Public School in Peshawar, Pakistan, in December 2014, are just some of the most egregious recent examples of the threat of violent extremism.

17. Violent extremists are also disrupting the day-to-day work of development actors, including United Nations development agencies and United Nations country teams, which are trying to help Member States eradicate poverty, and reduce social inequalities and exclusion. As a consequence, United Nations field personnel and peacekeepers have been targeted.

C. Human rights and the rule of law

18. Violent extremists pose a direct threat to the enjoyment of human rights, ranging from the right to life and the right to liberty and security of person, to freedom of expression, association, and thought, conscience and religion.

19. There is credible information indicating that terrorists and violent extremist groups like ISIL and its affiliates may have committed serious violations of international law, including genocide, crimes against humanity and war crimes. These groups also violate the rights of women and girls, including through sexual enslavement, forced marriages and encroachment on their rights to education and participation in public life. In areas where ISIL and other terrorist and violent extremist groups currently operate, it appears that religious communities, and women, children, political activists, journalists, human rights defenders and members of the lesbian, gay, bisexual, transgender and
intersex community are being systematically targeted, abducted, displaced and murdered. Torture, and sexual and gender-based violence, are also reportedly widespread. Items and sites of great historical, religious and cultural significance are being wantonly destroyed in violation of the protection afforded to the cultural heritage under international humanitarian law.

20. A lack of accountability in conflict areas is contributing to an increase in these atrocious crimes. Impunity and injustice create an environment of insecurity and helplessness, undermining conflict mediation and resolution efforts, including political transitions. We need to end impunity for all those committing violations and crimes, including crimes under international law. At the same time, we must be vigilant in ensuring that Member States’ efforts to address violent extremism are respectful of the rule of law and in accordance with their obligations under international human rights law, as well as international humanitarian law, if applicable. Certain rights are non-derogable even in time of public emergency which threatens the life of the nation.

D. Humanitarian action

21. At the end of 2014, the world was facing a situation where the number of forcibly displaced persons was the highest on record, a situation to which violent extremism was a significant contributing factor. It is not just the volume of displaced persons that is alarming, but also the rapid increase in their numbers, which has risen 40 per cent, from 42.5 million to 59.5 million in just three years. Internally displaced persons and refugees, particularly children, are at an increased risk of forced recruitment, including by violent extremist groups.

22. Violent extremist groups actively interfere with the provision of international humanitarian assistance, including food and vital medical aid, to populations in need by limiting the access of humanitarian actors to the areas controlled by those groups, or by seizing relief supplies. In situations of armed conflict, violent extremists routinely disregard the traditional protection, enshrined in international humanitarian law, accorded to humanitarian actors in conflict zones. As a result, many humanitarian workers have become targets themselves: 329 aid workers were killed, injured or kidnapped in 2014. While violent extremists groups are not the only actors using these despicable tactics, their growing influence is a significant contributory factor to the challenging operating environment confronted by humanitarian organizations.

III. Context and drivers of violent extremism

23. In the past decade and a half, research has been conducted on the drivers of violent extremism. However, there is no authoritative statistical data on the pathways towards individual radicalization. While there are some recognizable trends and patterns, there are only a few areas of consensus that exist among researchers. Qualitative research, based mainly on interviews, suggests that two main categories of drivers can be distinguished: “push factors,” or the conditions conducive to violent extremism and the structural context from which it emerges; and “pull factors,” or the individual motivations and processes, which play a key role in transforming ideas and grievances into violent extremist action. More research, both qualitative and quantitative, is required on this evolving phenomenon.

A. Conditions conducive to and the structural context of violent extremism

24. The available qualitative evidence points to the presence of certain recurrent drivers, which are common among a wide variety of countries and regions and which lead, sometimes in
isolation and sometimes in combination with other factors, to radicalization and violent extremism.

*Lack of socioeconomic opportunities*

25. Countries that fail to generate high and sustainable levels of growth, to create decent jobs for their youth, to reduce poverty and unemployment, to improve equality, to control corruption and to manage relationships among different communities in line with their human rights obligations, are more prone to violent extremism and tend to witness a greater number of incidents linked to violent extremism. Citizens may consider weak development outcomes as confirmation of the lack of a government’s legitimacy, making state institutions less effective in responding to violent extremism when it arises. The absence of alternative employment opportunities can make violent extremist organizations an attractive source of income.

*Marginalization and discrimination*

26. No country is completely homogeneous. Diversity in and of itself does not lead to or increase a country’s vulnerability to violent extremism. However, when a country experiences insecurities such as scarce resources, and when one group, whatever its demographic weight, acts monopolistically in political and economic sectors at the expense of other groups, the potential for intercommunal tensions, gender inequality, marginalization, alienation and discrimination increases, as expressed through restricted access to public services and job opportunities and obstructions to regional development and freedom of religion. This, in turn, may incite those who feel disenfranchised to embrace violent extremism as a vehicle for advancing their goals.

*Poor governance, violations of human rights and the rule of law*

27. Violent extremism tends to thrive in an environment characterized by poor governance, democracy deficits, corruption and a culture of impunity for unlawful behaviour engaged in by the State or its agents. When poor governance is combined with repressive policies and practices which violate human rights and the rule of law, the potency of the lure of violent extremism tends to be heightened. Violations of international human rights law committed in the name of state security can facilitate violent extremism by marginalizing individuals and alienating key constituencies, thus generating community support and sympathy for and complicity in the actions of violent extremists. Violent extremists also actively seek to exploit state repression and other grievances in their fight against the state. Thus, Governments that exhibit repressive and heavy-handed security responses in violation of human rights and the rule of law, such as profiling of certain populations, adoption of intrusive surveillance techniques and prolongation of declared states of emergency, tend to generate more violent extremists. International partners that are complicit in such action by States further corrupt public faith in the legitimacy of the wider international system.

28. The lack of adequate efforts, in line with international obligations, towards the realization of economic, social and cultural rights, exacerbated by discrimination against ethnic, national, gender, racial, religious, linguistic and other groups and the absence or curtailment of democratic space, can provide opportunities for exploitation by violent extremists. State institutions that do not adequately fulfil their international obligations to uphold these rights can fuel grievances and undermine not only their own effectiveness but also social norms and social cohesion.
29. In addition, more attention needs to be paid to devising efficient gender- and human rights-compliant reintegration strategies and programmes for those who have been convicted of terrorism-related offences as well as returning foreign terrorist fighters.

**Prolonged and unresolved conflicts**

30. Prolonged and unresolved conflicts tend to provide fertile ground for violent extremism, not only because of the suffering and lack of governance resulting from the conflict itself but also because such conflicts allow violent extremist groups to exploit deep-rooted grievances in order to garner support and seize territory and resources and control populations. Urgent measures must be taken to resolve protracted conflicts. Resolving these conflicts will undermine the impact of the insidious narratives of violent extremist groups. When prevention fails, our best strategy towards securing lasting peace and addressing violent extremism entails inclusive political solutions and accountability.

**Radicalization in prisons**

31. Research shows that harsh treatment in detention facilities can play a disconcertingly powerful role in the recruitment of a large number of individuals who have joined violent extremist groups and terrorist organizations. Several factors have been identified as spurring prisoners to seek protection by joining groups, including inhumane prison conditions and inhumane treatment of inmates, corrupt staff and security officers, gang activity, drug use, lack of security and proper facilities, and overcrowding. Safeguards need to be put in place to prevent the spread of extremist ideologies to other prisoners while upholding the protection afforded under international law to persons deprived of their liberty, including with respect to international standards and norms relating to solitary confinement.

**B. Processes of radicalization**

32. Although the conditions conducive to violent extremism affect entire populations, only a small number of individuals are actually radicalized and turn to violence. Both complex individual motivations and human agency play a key role in exploiting these conditions and transforming ideas and grievances into violent action.

**Individual backgrounds and motivations**

33. A negative personal experience which resonates with the narrative of violent extremist ideologies can heighten the chances that an individual will embrace violent extremism. Individual motivations vary from the serious to the routine: researchers have reported precipitating events as diverse as experiencing or witnessing torture, the death of a relative or friend at the hands of the security forces or a foreign power, unfair trials, the loss of property and the humiliation of a parent — and even the refusal of a personal loan.

34. While some highly educated individuals have played consequential roles in violent extremist organizations, many members are poorly educated, often not having completed secondary education. A large number have only rudimentary literacy levels and almost no religious knowledge or education, making them vulnerable to indoctrination. It is quite likely that they may have been engaged in petty crimes and illicit activities prior to their involvement with violent extremist groups. Membership in a group also promotes a sense of belonging or relief from the burden of alienation, isolation or anomie.
Collective grievances and victimization

35. Historical legacies of, or collective grievances stemming from, domination, oppression, subjugation or foreign intervention can enable narratives of victimization to take hold. These narratives can provoke simple and powerful emotional reactions which may then be exploited by violent extremists: the memory of past or present actual or perceived oppressions is upheld so as to fuel the thirst for revenge against oppressors.

Distortion and misuse of beliefs, political ideologies and ethnic and cultural differences

36. Violent extremist groups cynically distort and exploit religious beliefs, ethnic differences and political ideologies to legitimize their actions, establish their claim on territory and recruit followers. Distortion and misuse of religion are utilized to divide nations, cultures and people, undermining our humanity. Faith and community leaders are critical in mentoring vulnerable followers so as to enable them to reject violent ideologies and in providing opportunities for intra- and interfaith dialogue and discussion as a means of promoting tolerance, understanding and reconciliation between communities. Leaders, Governments, the international community and the media have to work together to prevent confrontation and polarization within and between countries, faiths, nations and peoples. We have to work jointly to halt this vicious cycle of provocation and response which often fuels the forces governing the nexus between conflict, terrorism and violent terrorism, as seen in Afghanistan, Iraq, Libya, the Syrian Arab Republic, Yemen and other countries.

Leadership and social networks

37. While contextual factors, personal experiences and collective grievances can all contribute to the emergence of violent extremism, there must also be a social context that provides some form of organization and direction for these elements. This is often established through the intervention of a charismatic leader or political entrepreneur, and through informal family and social networks. It can be difficult to join violent extremist organizations unless you already know one of their members, this being an inevitable consequence of the fact that their activities are often exclusive and clandestine. However, in recent years, online tools have served as an additional, and more accessible, pathway to group membership.

IV. An Agenda for Action: recommendations on preventing violent extremism

38. I have consistently called for the balanced implementation of the United Nations Global Counter-Terrorism Strategy. While we need to continue our concerted efforts to counter violent extremism, we have to broaden our responses, engage earlier and address the drivers of violent extremism. We need to complement the countering of violent extremism with preventive measures. Making prevention an integral part of our comprehensive approach will help us tackle many of the underlying conditions that drive individuals to join violent extremist groups. As with the practice of prevention more generally, results may not be visible immediately and will require our long-term and patient engagement.

39. I therefore put forward for the consideration of Member States the following recommendations, which I believe will prevent and reduce the space for violent extremism while simultaneously addressing the immediate peace and security challenges through ongoing counter-terrorism measures. My recommendations identify actions that can be taken at the global, national and regional levels with a view to promoting a comprehensive and balanced implementation of the United Nations Global Counter-Terrorism Strategy.
A. Setting the policy framework

A global framework for preventing violent extremism

40. Preventing violent extremism is a commitment and obligation under the principles and values enshrined in the Charter of the United Nations, the Universal Declaration of Human Rights [General Assembly Resolution 217A (III)] and other international human rights instruments. To be effective and sustainable and in line with Member States’ obligations under international law, all legislation, policies, strategies and practices adopted to prevent violent extremism must be firmly grounded in the respect for human rights and the rule of law.

41. Both the General Assembly and the Security Council have acknowledged that violent extremism has reached a level of threat and sophistication that requires concerted action beyond law enforcement, military or security measures to address development, good governance, human rights and humanitarian concerns. Strengthening the rule of law, repealing discriminatory legislation and implementing policies and laws that combat discrimination, marginalization and exclusion in law and in practice must be an essential component of any response to the threat posed by violent extremism.

42. In the past two years, the General Assembly has emphasized the need for united action on violent extremism: in the fourth review of the United Nations Global Counter-Terrorism Strategy; [See General Assembly resolution 68/276. Jin Assembly resolution 68/127, entitled “A world against violence and violent extremism”; and during the high-level thematic debate of the Assembly on the topic “Promoting tolerance and reconciliation: fostering peaceful, inclusive societies and countering violent extremism,” convened by the President of the Assembly in conjunction with the Secretary-General and the United Nations Alliance of Civilizations and held on 21 and 22 April 2015, as well as in the recent general debate of the Assembly at its seventieth session. The Security Council emphasized the need for measures to address violent extremism and stem the flow of foreign terrorist fighters in its resolution 2178 (2014), during the high-level open debate of the Council on the topic “The role of youth in countering violent extremism and promoting peace,” held on 23 April 2015, and in the statement by the President of the Council of 29 May 2015 (S/PRST/2015/11).

43. While we can set parameters at the global level, it is action at the local, national and regional levels that will have the most impact. I therefore count on Member States to translate our common commitment and political will to effect real change into new ways of formulating public policy so as to prevent violent extremism in their respective countries and regions. The Charter of the United Nations, the Universal Declaration of Human Rights and Member States’ obligations under international law — in particular under international human rights law, refugee law and, if applicable, international humanitarian law — provide a strong foundation, and the United Nations Global Counter-Terrorism Strategy and the guiding principles for counter-terrorism strategies, as identified at the International Conference on National and Regional Counter-Terrorism Strategies, held in Bogota from 31 January to 1 February 2013, provide additional guidance for national and regional plans of action. The processes for establishing national plans and regional strategies or refining existing ones should complement both the present Plan of Action and each other. The United Nations, through the 36 entities of the Counter-Terrorism Implementation Task Force and an “All United Nations” approach, is ready to support Member States in developing such policies and plans. I will also direct resident coordinators, United Nations country teams and the regional United Nations Development Group teams to support Member States, upon their request, in developing their plans at the national and regional levels.
National plans of action for preventing violent extremism

44. Each Member State should consider developing a national plan of action to prevent violent extremism which sets national priorities for addressing the local drivers of violent extremism and complements national counter-terrorism strategies where they already exist. Based on the principle of national ownership and in accordance with international law, Member States may wish to consider the following elements in establishing such plans:

(a) National plans should be developed in a multidisciplinary manner, to include countering and preventing violent extremism measures, with input from a wide range of government actors, such as law enforcement, social service providers and ministries of education, youth and religious affairs, as well as non-governmental actors, including youth; families; women; religious, cultural and educational leaders; civil society organizations; the media; and the private sector. Analyses of local and national drivers of violent extremism form an important point of departure for developing national plans;

(b) National plans should fortify the social compact against violent extremism by promoting respect for the principle of equality before the law and equal protection under the law in all government-citizen relations, and developing effective, accountable and transparent institutions at all levels, as well as ensuring responsive, inclusive, participatory and representative decision-making. I encourage parliamentarians to provide the legislative foundation for national plans of action for preventing violent extremism consistent with their national and international obligations, where necessary;

(c) National plans should address the issue of foreign terrorist fighters, as called for in Security Council resolution 2178 (2014). In that resolution, the Council decided that States should ensure that their legal systems provide for the prosecution of travel for terrorism or related training; and that States should also address the financing or facilitation of such activities and prevent entry or transit through their territories, including through the usage of internationally accepted databases, of any individual with respect to whom there is credible information that provides reasonable grounds for believing that this travel is undertaken for the purpose of participating in a terrorist act. The guiding principles on stemming the flow of foreign terrorist fighters agreed at the special meeting of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism, held in Madrid on 28 July 2015, could be useful in this regard;

(d) National plans should prevent violent extremist and terrorist groups from trading in oil and antiquities, hostage-taking, and receiving donations, in line with Member States’ obligations under Security Council resolution 2199 (2015);

(e) One means of addressing many of the drivers of violent extremism will be to align national development policies with the Sustainable Development Goals, specifically ending poverty in all its forms everywhere (Goal 1); ensuring inclusive and equitable quality education and promoting lifelong learning opportunities for all (Goal 4); achieving gender equality and empowering all women and girls (Goal 5); promoting sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all (Goal 8); reducing inequality within and among countries (Goal 10); making cities and human settlements inclusive, safe, resilient and sustainable (Goal 11); and promoting peaceful and inclusive societies for sustainable development, providing access to justice for all and building effective, accountable and inclusive institutions at all levels (Goal 16);

(f) National plans should dedicate funding for implementation by government and non-governmental entities and promote public-private partnerships, where applicable;

(g) Effective monitoring and evaluation mechanisms for these plans are essential to ensuring that policies are having the desired impact.
Regional plans of action to prevent violent extremism

45. As violent extremism does not respect borders, national and global action has to be complemented by enhanced regional cooperation. Several subregions and regions have already adopted comprehensive counter-terrorism strategies. Member States should come together to complement those strategies or adopt new regional or subregional plans of action to prevent violent extremism, facilitated by regional or subregional organizations and the United Nations, with a view to complementing and reinforcing their national plans. To this end, Member States should:

(a) Strengthen subregional and regional organizations, including by creating and maintaining regional contact lists of focal points, monitoring the trafficking of small arms and heavy weapons, and facilitating intergovernmental communication and cooperation. Establishing early warning centres for the exchange of information on violent extremist activities could render this interaction more predictable and could thus be of additional value;
(b) Enable subregional and regional organizations to provide technical assistance to Member States in the respective subregion or region in building capacity for preventing violent extremism and support effective cooperation, for example, on border management.

Mobilizing resources

46. To transform our commitment into lasting change, we need to make more efficient use of existing funds and consider how, based on the interdependence of political, social and economic drivers of violent extremism, we can create synergies in our resource allocation. Moreover, within the peace and security sector, there is a growing understanding that many preventive measures, traditionally understood to be part of development efforts, can help address these drivers. The newly adopted Sustainable Development Goals explicitly include goals and targets related to preventing violence and promoting peaceful and inclusive societies.

47. Investment in prevention is far more cost-effective than allocating resources to mitigating consequences. I therefore recommend considering:

(a) Adjusting the focus of existing funds dedicated to countering terrorism and violent extremism to enable them to also address the drivers of violent extremism, and thereby ultimately using available resources more effectively;
(b) Identifying other funding sources across sectors and evaluating how Governments and regional and international institutions could adapt existing funds so as to expand programming that is sensitive to preventing violent extremism.

B. Taking action

48. In developing national plans of action and regional strategies, Member States should consider addressing the elements outlined below.

Dialogue and conflict prevention

49. In my report to the Security Council entitled “The United Nations and conflict prevention: a collective recommitment” (S/2015/730), I noted that the risk of violent extremism often increases in the same conditions that lead to heightened risk of conflict. Where conflict already exists, we must redouble our efforts to promote and sustain dialogue between warring parties, since persistent unresolved conflict is proving to be a major driver of violent extremism. While we may benefit in these situations from using some of the tools already developed to prevent
conflict, we have also started developing specific initiatives for the prevention of violent extremism through the Counter-Terrorism Implementation Task Force and the United Nations Counter-Terrorism Centre, such as a Task Force working group on the prevention of violent extremism and a Task Force working group on the conditions conducive to the spread of terrorism and a regional youth engagement and skills development programme. I therefore recommend that Member States:

(a) Ensure that, in circumstances where military action becomes necessary to counter the expansion of violent extremist groups, any such response is in full compliance with international law, in particular with the Charter of the United Nations, international human rights law, international refugee law and international humanitarian law;
(b) Engage opposing parties and regional actors earlier on and seek to forge international consensus so as to give regional and United Nations diplomacy the leverage that it needs to broker solutions. Delaying engagement reduces options, and increases financial and human costs;
(c) Encourage individuals to leave violent extremist groups by developing programmes that place an emphasis on providing them with educational and economic opportunities. To avert perceptions of injustice which might result from extending assistance to these perpetrators, such programmes should not draw from initiatives addressing the needs of the wider civilian population;
(d) Explore opportunities to introduce alternative dispute resolution mechanisms, such as mediation, arbitration and restorative justice, to resolve conflict and achieve sustainable peace;
(e) Engage religious leaders to provide a platform for intra- and interfaith dialogue and discussions through which to promote tolerance and understanding between communities, and voice their rejection of violent doctrines by emphasizing the peaceful and humanitarian values inherent in their theologies. Religious leaders also have a responsibility to themselves to seek such understanding. Tolerance is not passive: it demands the active choice to reach out on a basis of mutual understanding and respect, especially where disagreement exists;
(f) Preserve the heritage of cultural and religious diversity against the attempts by violent extremists to destroy manuscripts, objects and sites that are symbols of pluralism and tolerance;
(g) Convene regional and national dialogues on preventing violent extremism with a range of actors, encompassing youth engagement, gender equality, the inclusion of marginalized groups, the role of municipalities, and positive outreach through social media and other virtual platforms.

Strengthening good governance, human rights and the rule of law

50. When Governments embrace international human rights norms and standards, promote good governance, uphold the rule of law and eliminate corruption, they create an enabling environment for civil society and reduce the appeal of violent extremism. Policies and initiatives that are firmly grounded in human rights are essential to ensuring the inclusion of individuals or communities that are vulnerable to violent extremism. We need to find ways to strengthen trust between government institutions and communities to prevent real or perceived marginalization and exclusion. I therefore recommend that Member States:

(a) Review all national legislation, policies, strategies and practices aimed at preventing and countering violent extremism to ascertain whether they are firmly grounded in respect for human rights and the rule of law, and whether they put in place national mechanisms designed to ensure compliance. This may also involve taking measures to strengthen the rule of law, repealing discriminatory legislation and implementing policies and laws that combat discrimination and exclusion;
(b) Provide access to justice for all and strengthen fair, effective, accountable and inclusive institutions at all levels, in line with the 2030 Agenda for Sustainable Development;
(c) Foster non-discriminatory basic service provision, ensure accountability for service delivery, and extend state services to remote areas and create an environment where entrepreneurship can flourish and societies can become more peaceful, just and inclusive;
(d) Strengthen the professionalism of security forces, law enforcement agencies and justice institutions; and ensure effective oversight and accountability of such bodies, in conformity with international human rights law and the rule of law. This may involve providing dedicated human rights training to security forces, law enforcement agents and all those involved in the administration of justice regarding the prohibition of incitement to hatred and, more broadly, respect for human rights within the context of measures taken to counter violent extremism and terrorism;
(e) Ensure accountability for gross violations of international human rights law and international humanitarian law, including those amounting to crimes under international law, such as war crimes and crimes against humanity, through criminal procedures adhering to due-process guarantees. Accountability mechanisms should have relevant gender expertise to fulfil their mandates. In cases where national procedures are not able or are unwilling to address such crimes, the international community should support accountability efforts, including through a referral of such situations by the Security Council to the International Criminal Court or to an ad hoc tribunal, where appropriate;
(f) Reform national legal frameworks and penitentiary systems to ensure the security of inmates, personnel and facilities and establish procedures to prevent and counter radicalization in prisons based on human rights and the rule of law;
(g) Introduce disengagement, rehabilitation and counselling programmes for persons engaged in violent extremism which are gender-sensitive and include programmes for children to facilitate their reintegration into society. These programmes must be in full compliance with international human rights norms and standards, including the rights to freedom of movement, freedom of expression and privacy, gender equality and the principle of non-discrimination;
(h) Promote the enjoyment of economic, social and cultural rights, including through human rights-based initiatives that help eliminate the conditions conducive to violent extremism. Such programmes can be particularly helpful when one group, whatever its demographic weight, behaves monopolistically in the political and economic sectors at the expense of other groups;
(i) Implement Security Council resolution 1624 (2005), promoting a comprehensive approach to incitement and violent extremism, and the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (A/HRC/22/17/Add.4, appendix), involving all relevant actors, such as national human rights institutions, civil society, political parties and the media;
(j) Prevent the subversion of the work of educational, cultural and religious institutions by terrorists and their supporters, as highlighted in Security Council resolution 1624 (2005); take appropriate measures against all forms of intolerance and discrimination based on religion or belief, as exhibited in particular in the curricula of formal and non-formal educational institutions, and textbooks and teaching methods;
(k) Ensure that any restrictions on freedom of expression are clearly and narrowly defined and meet the three-part test of legality, proportionality and necessity.

**Engaging communities**

51. For their survival, violent extremists require the tacit support of a wider circle of sympathizers. If violent extremists can be deprived of this support, their capacity to cause harm and evade justice will be greatly reduced. While engagement with communities marked by a long history of distrust of the government can pose a challenge, there are a number of
community engagement strategies that hold promise. I therefore recommend that Member States:

(a) Develop joint and participatory strategies, including with civil society and local communities, to prevent the emergence of violent extremism, protect communities from recruitment and the threat of violent extremism, and support confidence-building measures at the community level by providing appropriate platforms for dialogue and the early identification of grievances;

(b) Adopt community-oriented policing models and programmes that seek to solve local issues in partnership with the community and are firmly based on human rights so as to avoid putting community members at risk. This would increase public awareness and vigilance and improve police understanding and knowledge with regard to communities, thus enhancing their ability to be proactive and identify grievances and critical issues at an early stage;

(c) Develop local and family-based mentorship programmes, based on a one-to-one relationship between mentor and mentee, focusing on vulnerable individuals or those who have been convicted of or charged with criminal acts related to violent extremism;

(d) Provide medical, psychosocial and legal service support in communities that give shelter to victims of violent extremists, including victims of sexual and gender-based crimes;

(e) Encourage civic and professional associations, unions and chambers of commerce to reach out through their own networks to marginalized groups so as to address challenges together through inclusive dialogue and consensual politics;

(f) Support the establishment of regional and global networks for civil society, youth, women’s organizations and religious leaders to enable them to share good practices and experience so as to improve work in their respective communities and promote intercultural and interfaith dialogue;

(g) Promote, in partnership with civil society and communities, a discourse that addresses the drivers of violent extremism, including ongoing human rights violations. Address any existing human rights violations, as a matter of both legal obligation and credibility.

Empowering youth

52. We must pay particular attention to youth. The world’s 1.8 billion young women and men constitute an invaluable partner in our striving to prevent violent extremism. We have to identify better tools with which to support young people as they take up the causes of peace, pluralism and mutual respect. The rapid advance of modern communications technology also means that today’s youth form a global community of an unprecedented kind. This interconnectivity is already being exploited by violent extremists; we need to reclaim this space by helping to amplify the voices of young people already promoting the values of mutual respect and peace to their peers. I therefore recommend that Member States:

(a) Support and enhance young women’s and young men’s participation in activities aimed at preventing violent extremism by prioritizing meaningful engagement mechanisms at the national, regional and global levels, as laid out in the 2015 Amman Declaration on Youth, Peace and Security; and provide a physically, socially and emotionally safe and supportive environment for the participation of young women and men in preventing violent extremism;

(b) Integrate young women and men into decision-making processes at local and national levels, including by establishing youth councils and similar mechanisms which give young women and men a platform for participating in mainstream political discourse;

(c) Foster trust between decision makers and young women and men, especially through intergenerational dialogue and youth-adult confidence-building activities and training;
(d) Involve hard-to-reach young women and men, such as those from underrepresented groups, in efforts to prevent violent extremism, as laid out in the Guiding Principles on Young People’s Participation in Peacebuilding;
(e) Establish national mentoring programmes for young women and men, create space for personal growth in their chosen fields, and offer opportunities for community service which can enable them to become leaders and actors for constructive change;
(f) Ensure that a portion of all funds dedicated to addressing violent extremism are committed to projects that address young people’s specific needs or empower them and encourage international financial institutions, foundations and other donors to provide small grant funding mechanisms to women and young social entrepreneurs to enable them to develop their own ideas on strengthening community resilience against violent extremism.

**Gender equality and empowering women**

53. Women’s empowerment is a critical force for sustainable peace. While women do sometimes play an active role in violent extremist organizations, it is also no coincidence that societies for which gender equality indicators are higher are less vulnerable to violent extremism. We must therefore ask ourselves how we can better promote women’s participation, leadership and empowerment across society, including in governmental, security sector and civil society institutions. In line with Security Council resolution 2242 (2015), we must ensure that the protection and empowerment of women is a central consideration of strategies devised to counter terrorism and violent extremism. There is also a need to ensure that efforts to counter terrorism and violent extremism do not impact adversely on women’s rights. I therefore recommend that Member States:

(a) Mainstream gender perspectives across efforts to prevent violent extremism;
(b) Invest in gender-sensitive research and data collection on women’s roles in violent extremism, including on identifying the drivers that lead women to join violent extremist groups, and on the impacts of counter-terrorism strategies on their lives, in order to develop targeted and evidence-based policy and programming responses;
(c) Include women and other underrepresented groups in national law enforcement and security agencies, including as part of counter-terrorism prevention and response frameworks;
(d) Build the capacity of women and their civil society groups to engage in prevention and response efforts related to violent extremism;
(e) Ensure that a portion of all funds dedicated to addressing violent extremism are committed to projects that address women’s specific needs or empower women, as recommended in my recent report to the Security Council on women and peace and security (S/2015/716).

**Education, skills development and employment facilitation**

54. As part of the struggle against poverty and social marginalization, we need to ensure that every child receives a quality education which equips him or her for life, as stipulated under the right to education. Education should include teaching respect for human rights and diversity, fostering critical thinking, promoting media and digital literacy, and developing the behavioural and socioemotional skills to contribute to peaceful coexistence and tolerance. Young women and men entering the workplace need our support — both in gaining access to continued learning and vocational resources, and in incubating their entrepreneurial talent. I therefore recommend that Member States:
(a) Invest in education, in particular early childhood education, from ages 3 to 8, to ensure that all children have access to inclusive, high-quality education, taking into account diverse social and cultural settings;
(b) Implement education programmes that promote “global citizenship,” soft skills, critical thinking and digital literacy, and explore means of introducing civic education into school curricula, textbooks and teaching materials. Build the capacity of teachers and educators to support this agenda;
(c) Provide comprehensive primary through tertiary education, including technical and vocational education, and mentoring for all vulnerable people, including the displaced, by leveraging online and mobile technology;
(d) Collaborate with local authorities to create social and economic opportunities, in both rural and urban locations; invest in equipping people with the skills needed to meet local labour demands through relevant education opportunities;
(e) Provide young people with additional career options by fostering an entrepreneurial culture and offering entrepreneurship education, facilitating employment searches and job-matching, enacting regulations to promote the development of micro and small enterprises, easing access to finance and microcredit and increasing the range of support services such as marketing and distribution, so as to unleash the full economic potential of youth;
(f) Invite the private sector and other civil society actors to contribute to post-conflict reconciliation and reconstruction efforts, especially job creation, facilitation and training opportunities.

Strategic communications, the Internet and social media

55. The manipulative messages of violent extremists on social media have achieved considerable success in luring people, especially young women and men, into their ranks. While violent extremists have demonstrated some sophistication in their use of old and new media tools, it is equally true that we who reject their message have largely failed to communicate to those who are disillusioned and disenfranchised a vision of the future that captures their imagination and offers the prospect of tangible change. Thousands of young activists and artists are fighting back against violent extremism online through music, art, film, comics and humour, and they deserve our support. I therefore recommend that Member States:

(a) Develop and implement national communications strategies, in close cooperation with social media companies and the private sector, that are tailored to local contexts, gender sensitive and based on international human rights standards, to challenge the narratives associated with violent extremism;
(b) Encourage more research on the relationship between the misuse of the Internet and social media by violent extremists and the factors that drive individuals towards violent extremism;
(c) Promote grass-roots efforts to advance the values of tolerance, pluralism and understanding;
(d) Ensure that national legal frameworks protect freedom of opinion and expression, pluralism, and diversity of the media;
(e) Empower and enable victims to transform their loss and suffering into a constructive force for preventing violent extremism by providing them with online forums where they can tell their stories;
(f) Protect journalists, who play a crucial role in democratic societies, by ensuring the prompt and thorough investigation of threats to their safety, and encourage journalists to work together to voluntarily develop media training and industry codes of conduct which foster tolerance and respect.
C. Supporting Member States, regional bodies and communities through the United Nations

56. The primary responsibility for preventing violent extremism rests with Member States. As they develop their response, the United Nations can act as a natural partner. The United Nations can help foster global dialogue, uniting countries, people and communities on the basis of universally shared values and principles as enshrined in international law, including human rights instruments.

57. In cooperation with Member States, United Nations missions, programmes and projects are already addressing the underlying drivers and triggers of violent extremism. Violent extremist groups, which recognize the power of these tools, are targeting peacekeepers, human rights advocates, educators, civil society activists and aid workers in order to weaken our resolve and our results. We need to be more strategic and better coordinated in our activities in order to enhance coherence across the full spectrum of security, sustainable development, human rights and humanitarian assistance. This will require that United Nations peace and security efforts and sustainable development policy frameworks address the drivers of violent extremism, that we further strengthen the promotion and protection of fundamental human rights and the rule of law and that humanitarian principles are respected, that humanitarian actors have the necessary space within which to operate and that our humanitarian work is people-centred, supports resilient communities and does not fuel conflict.

58. I have instructed United Nations entities to redouble their efforts in coordinating and developing activities with Member States, to prioritize, sensitize and adapt existing programmes to permit them to target the drivers of violent extremism more precisely and to introduce new initiatives to close potential gaps. I therefore intend to:

(a) Adopt an All-of-UN approach to supporting national, regional and global efforts to prevent violent extremism through the United Nations Chief Executives Board for Coordination, as well as through existing United Nations inter-agency bodies and the Counter-Terrorism Implementation Task Force and its entities, which bear the primary responsibility for supporting Member States in implementing all four pillars of the United Nations Global Counter-Terrorism Strategy. By adopting an All-of-UN approach through the Task Force framework, the Organization will coordinate its action more closely and help channel and share initiatives that have proved effective;

(b) Integrate preventing violent extremism into relevant activities of United Nations peacekeeping operations and special political missions in accordance with their mandates, as well as into relevant activities of United Nations country teams in order to build the capacity of Member States through such mechanisms as the United Nations Development Assistance Frameworks, the United Nations common country assessments, youth advisory Boards, the Global Focal Point for Police, Justice and Corrections, and disarmament, demobilization and reintegration and security sector reform programming;

(c) Encourage United Nations governing and executive boards to enhance the capacities of United Nations agencies, funds and programmes to support Member States in developing and implementing their national plans of action for preventing violent extremism;

(d) Offer capacity-building programmes aimed at strengthening national and regional capacities to develop institutional plans designed to prevent violent extremism and share good practices, and assist Member States in adopting relevant legislation and policies in close coordination with the relevant United Nations country teams, special representatives of the Secretary-General, peace operations where deployed, and entities of the Counter-Terrorism Implementation Task Force, including the Counter-Terrorism Committee Executive Directorate, the Office of the United Nations High Commissioner for Human Rights, the United Nations Interregional Crime and Justice Research Institute, the United Nations Office on Drugs and Crime and the United Nations Counter-Terrorism Centre;
(e) Launch a United Nations global communications strategy to prevent violent extremism, grounded in United Nations core values of peace, justice, tolerance and human dignity as they are enshrined in the Charter of the United Nations, the Universal Declaration of Human Rights and other instruments, reinforcing these shared values around the world and supporting Member States in tailoring their own national and local communication strategies, upon their request;

(f) Further strengthen early and effective action through the Human Rights Upfront Initiative to prevent or respond to large-scale violations of international human rights law or international humanitarian law, at both the policy and the operational level;

(g) Develop a standing United Nations prevention of violent extremism platform to direct the implementation of this Plan, facilitated by the Counter-Terrorism Implementation Task Force and supported by the United Nations Counter-Terrorism Centre. This platform would coordinate policy within the United Nations system and support Member States in developing their institutional responses to violent extremism at the local, national and regional levels by sharing lessons learned. It should foster cooperation between Member States, including through South-South and triangular partnerships;

(h) Support Governments seeking to develop and implement education programmes that promote civic education, soft skills, critical thinking, digital literacy, tolerance and respect for diversity, including, for example, peace education modules for the use of school-age children, in order to promote the culture of non-violence;

(i) Launch a global awareness campaign to support victims of violent extremism and provide them with a global platform within which to share their stories by expanding the Victims of Terrorism Support Portal;

(j) Encourage youth exchange programmes within and among Member States, which could be further developed into global community service and global youth programmes to enhance cross-cultural understanding, promote learning of new skills and support development initiatives;

(k) Invite relevant private actors, including communications and social media companies, to support the prevention of violent extremism initiatives and generate creative ideas to help the international community effectively address the spread of violent extremism through the Internet;

(l) Develop a proposal for a Secretary-General’s fund to support innovative projects aimed at preventing violent extremism, especially in the fields of communications and community empowerment.

V. An appeal for concerted action

59. Undermining our common humanity, violent extremism is inherently global. It is driven by a mixture of personal, societal and ideational factors whose manifestations vary from one individual to the next. Violent extremism has affected different societies during different eras and in different regions of the world. The present plan of action does not provide a single solution to this challenge — there is no one tool or approach that will put it to rest forever. Instead, we need to broaden the way we think about this threat and take measures to prevent it from proliferating. What is most alarming in the present context is the rapid expansion of violent extremist ideologies in different parts of the world, which is being facilitated by the technological revolution. In the true spirit of the Charter of the United Nations, we must take action now in order to save succeeding generations.

60. To be effective in preventing violent extremism, our actions have to be as agile and far-reaching as the phenomenon itself. We have to improve our set of tools dynamically and keep reviewing our responses. The Plan of Action constitutes the inaugural basis for a comprehensive approach to this fast evolving, multidimensional challenge. I have asked my
staff to keep the action of the United Nations under constant review and to provide me with updates regarding what we might also be doing.

61. I am convinced that unity in principled action will overcome the rhetoric and appeal of violent extremism and, ultimately, the violent extremist groups themselves. At a time of growing polarization on a number of national, regional and global issues, preventing violent extremism offers a real opportunity for the members of the international community to unite, harmonize their actions and pursue inclusive approaches in the face of division, intolerance and hatred.

62. The General Assembly is the only body that can speak with a global voice to all parts of the world where violent extremists seek to spread intolerance and division. I therefore call upon all Member States to use that voice to send forth a resounding appeal for unity and action.
Endnotes

1 The UN Secretary-General presented this plan to the General Assembly in late 2015.
2 Eric Rosand and Alastair Millar, “Where is UN Counter-Terrorism Heading 20 Years after 9/11?” IPI Global Observatory, 26 February 2021. Available at: https://theglobalobservatory.org/2021/02/where-is-un-counterterrorism-headed-20-years-after-9-11/.

3 One study from 2019, surveying 111 key publications of the existing literature concluded: “The results of this scoping review of P/CVE interventions show that at the moment there are no evidence-based interventions that prevent and counter the development of the intention to commit acts of violent extremism, at least not according to the definition of an “evidence-based intervention” suggested in this review. This conclusion is motivated by the lack of studies evaluating the comparative effectiveness of the outcomes of interventions relevant to P/CVE.” (…) ‘In the included literature, two publications measured the comparative effectiveness of interventions. The results of these studies imply that educational interventions increase knowledge about, and change attitudes towards, violent extremism. No studies evaluating outcomes of the comparative effectiveness of interventions relevant to preventing or countering the development of the intention to commit violent extremism were found in the literature.” – Pistone, Isabella et al. (2019, Summer): “A Scoping Review of Interventions for Preventing and Countering Violent Extremism: Current Status and Implications for Future Research”. Journal for Deradicalization 19, p. 25 and p. 25. Available at: http://journals.sfu.ca/jd/index.php/jd/article/view/213.


5 UN General Assembly, United Nations Global Counter-Terrorism Strategy, A/RES/60/288, 20 September 2006 (adopted 8 September 2006) The first of four pillars of the Global Counter-Terrorism Strategy adopted by the General Assembly in 2006 covers measures to address the conditions conducive to the spread of terrorism; the second pillar, measures to prevent and combat terrorism; pillar three, measures to build States’ capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard; and pillar four, measures to facilitate the promotion and protection of human rights for all and the rule of law as the fundamental basis of the fight against terrorism. Available at: https://undocs.org/A/RES/60/288.


7 Ucko, David H., “Preventing violent extremism through the United Nations: The rise and fall of a good idea”. International Affairs 94 (2) February 2016, p. 260 [quoted from pre-print version].


10 However, in May 2021, the post-Trump US Department of Homeland Security established a new Center for Prevention Programs and Partnerships (CP3) which might also reinvigorate international efforts of terrorism prevention. Cf. 11 May 2021 Press Release “DHS Creates New Center for Prevention Programs and Partnerships and Additional Efforts to Comprehensively Combat Domestic Violent Extremism”. Available at: dhs.us.

11 Cf. Appendix to chapter 27.

12 Global Initiative against Transnational Organized Crime, (2021) The Global Illicit Economy: Trajectories of Transnational Organized Crime. Geneva: GIATOC, March 2021. Available at: https://globalinitiative.net/wp-content/uploads/2021/03/The-Global-Ilicit-Economy-GITOCPdf.pdf. One of the world’s most detailed monitoring project on conflicts, based in Heidelberg, Germany, and operating since 1991, arrived at different figures: it counted 40 wars – 21 full scale and 19 limited wars in 2020. The Heidelberg research team, monitoring also violent crises and non-violent conflicts, provided in its most recent report these figures: “In 2020, HIIK observed a total of 359 conflicts worldwide. About 60 percent, 220, were fought violently, while 139 were on a non-violent level. Compared to 2019, the overall number of full-scale wars increased from 15 to 21. The number of limited wars decreased from 23 to 19. (...) In 2020, HIIK observed 21 wars, six more than in the previous year. On par with 2014, this was the highest number of wars ever recorded by HIIK. Three limited wars escalated to full-scale wars. All three were located in Sub-Saharan Africa. Moreover, four violent crises escalated to wars. (...) The number of limited wars decreased by four from 23 in 2019 to 19 this year. Nine conflicts continued on the same level as in the previous year. Eight violent crises escalated to limited wars, while at the same time, ten limited wars de-escalated to the level of a violent crisis. Three limited wars escalated to full-scale wars, while two conflicts de-escalated from war-level to limited war-level.” Heidelberg

14 Chapter 4, Abstract.
15 Chapter 4, Conclusion.
16 Chapter 4, Abstract.
19 Th. Samuels, chapter 7.
27 Institute for Economics & Peace (IEP) Global Terrorism Index 2020: Measuring the Impact of Terrorism, Sydney, November 2020, pp. 67-68; Available at: https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf. However, the authors of this report stress that “…the correlations for developing countries are often different from the one found in countries with advanced economies. The authors also caution that “As it is a characteristic of systems analysis, the notion of [direction of – APS] causality is not always clear.” IEP, pp. 67-68.
28 IEP, p.3.
29 Point 10 of UN Plan of Action.
30 Source: Institute for Economics & Peace (IEP) Global Terrorism Index 2020, op. cit., p.68.
NEET stands for Youth Not in Education, Employment or Training.
31 IEP, p.68. - The IEP also noted that “There were 236,422 deaths from terrorism between 2002 and 2019. Of these deaths… 224,582, occurred in countries involved in conflict” (p. 41).

32 Ibid., p. 99: "Physical integrity is understood as freedom from political killings and torture by the government. (…) The index is based on indicators that reflect violence committed by government agents and that are not directly referring to elections”.

33 UN OCT, Reference Guide, op. cit., p.23. The unwillingness or inability of the drafters of the Plan of Action to define ‘violent extremism’ was one of the plan’s weaknesses. One astute observer of the UN, David H. Ucko, commented: “….the Plan of Action never defined “violent extremism,” but noted instead it “encompassed a wider category of manifestations” than terrorist acts. If making definitions “the prerogative of Member-States” was meant to avoid an endless, and perhaps fruitless, discussion of terminology, this so-called “practical approach” also had the effect of creating ambiguity, which greatly undercut the new concept. In the absence of definitions of violent extremism, member-states looked to the examples provided in the Plan, nearly all of which cited groups that self-identify as Islamic: IS, Al Qaeda, Boko Haram, and so on. (…) Instead, Egypt, Pakistan, and other members of the Organization of Islamic Cooperation (OIC) felt targeted and, in discussing the plan, repeatedly stressed the need to distance Islam from the conversation. In fact, the Plan of Action never mentions Islam, or the Muslim religion, and yet Islam appeared more than 40 times in the related GA discussion. In terms of achieving buy-in with the countries at the frontline of the counter-ideological struggle against violent Islamism, this was an own goal.” Ucko 2016, p. 265.

34 Cf. Chapter 2 of this Handbook for text of the draft definition of the Ad Hoc Committee of the 6th (legal) Committee of the UN General Assembly.


37 Cf. /RES/70/291, para 39,40, UN PVE Plan of Action, A/70/674, para 7, UN Secretary-General’s Statement at the first meeting of the High Level PVE Action Group on 27 October 2016; International Centre for Counter-Terrorism, 12 Principles for National Action planning, No. 2; cit. UN Office of Counter-Terrorism, Reference Guide, op. cit., p.10. [violent extremism, 21 July 2016 (A/HRC/33/29)].

38 Ucko 2016, p.252; comment by one of the drafters of the Plan of Action to author of this chapter.

39 Ibid., p...255.


41 David Ucko has pointed out that “It may just be telling that in listing the priorities of the new under-secretary-general of the UN Counter-Terrorism Office, PVE comes in at the fifth and final place.” Ucko 2016, p. 266.


43 Cf. Ucko, David J.: “…..many governments are deeply suspicious of civil society, and would actively resist any international effort to boost its power relative to the state. Even in elaborating the Plan of Action, drafters faced immediate problems with Russia wanting to
downplay the role of civil society and China resisting the language of human rights” (Ucko 2016, p. 267). Eric Rosand observed: “The UN General Assembly has only been able to “take note” of the Secretary-General’s PVE Plan of Action, with Egypt and Russia foremost among the nations preventing an endorsement of the framework. See, for example, the statement by Oleg Syromolotov, deputy minister of foreign affairs of the Russian Federation, at the OSCE Counter-Terrorism Conference in Rome, May 10, 2018, arguing that P/CVE is “pretext to interfere in the internal affairs of sovereign states and destabilize legitimate governments” (https://osce.mid.ru/web/osce-en/-/oleg-syromolotov-at-the-osce-counter-terrorism-conference).” Rosand, Eric. Preparing the Global Counterterrorism Forum for the Next Decade. Washington, DC: United States Institute of Peace. Special Report No. 476, August 2020, p. 22.

44 The Economist Group. Democracy Index 2019. London: The Economist Intelligence Unit, 2020, p. 3. The fact that not all 193 UN member states are covered by the survey (but only 167) is due to the fact that the 26 missing countries are small in terms of population. Therefore, the overall percentage distribution is not seriously affected. – On the decline of democracy in the 21st century, see also: Global Initiative against Transnational Organized Crime, (2021) The Global Illicit Economy: Trajectories of Transnational Organized Crime. Geneva: GITOC, March 2021. Available at: https://globalinitiative.net/wp-content/uploads/2021/03/The-Global-Illlicit-Economy-GITOC-Low.pdf


46 IEP, p.68-70.


50 Cf. Council of Europe. Counter-Terrorism Strategy (201802020). Available at: https://coe.int/cm/Pages/result_details.aspx?Objectid=0900000168afcpp


52 Council of Europe. *Counter-Terrorism Strategy* (201802020), pp. 3-4. Available at: https://coe.int/cm/Pages/result_details.aspx?Objectid=0900000168afcpr.


58 A similar plan was developed by the Abu-Dhabi-based think tank Hedayah. Its guidelines and good practices for developing national P/CVE strategies and action plans to facilitate implementation of the UN Plan of Action, included 14 steps:

1. Conduct an analysis of the threat;
2. Assess the current status of CVE strategies and policies that exist in that country;
3. Review the existing relevant research on violent extremism and CVE;
4. Review other existing national CVE strategies, good practices and lessons learned internationally to draw on the existing body of knowledge;
5. Identify the key actors and stakeholders to consult and involve throughout the process;
6. Create designated forum;
7. Create timeline for the development process of the strategy;
8. Set priorities for AVE activities and concrete measurable goals in alignment with existing good practice;
9. Determine budgetary resources and capacity (including staffing) needed, and assess availability;
10. Develop and disseminate the strategy document to all relevant stakeholders and partners;
11. Develop a strategic communications plan;
12. Review local push and pull factors, analysis of the threat, and strategy systematically and periodically;
13. Build local, particularly community-based awareness of the general violent extremist threat, to include recruitment narratives, techniques, and avenues of communication;


62 The UN Reference Guide. Developing National and Regional Action Plans to Prevent Violent Extremism. New York: UN, n.d.. It noted that “A one-size-fits-all model for a PVE plan does not exist.” (p.6)


65 Lawrence, Freedman, the author of Strategy (2013), made some important observations leading him to a short definition (below, at the end of this footnote). He started by observing that “...strategy remains the best word we have for expressing attempts to think about actions in advance, in the light of our goals and our capacities. (...) There is no agreed-upon definition of strategy that describes the field and limits its boundaries. One common contemporary definition describes it as being about maintaining a balance between ends, ways and means; about identifying objectives; and about the resources and methods available for meeting such objectives. (...) By and large, strategy comes into play where there is actual or potential conflict, when interests collide and forms of resolution are required. This is why strategy is more than a plan. (...) Strategy is often expected to start with a description of a desired end state, but in practice there is rarely an orderly movement to goals set in advance. (...) …the realm of strategy is one of bargaining and persuasion as well as threats and pressure, psychological as well as physical effects, and words as well as deeds. This is why strategy is the central political art. It is about getting more out of a situation than the starting balance of power would suggest. It is the art of creating power”. - Lawrence Freedman. Strategy. Oxford: Oxford University Press, 2006, pp. x-xii, pp.72-75, p. 88, pp. 607-608

66 Gregory Miller is Professor of Strategy at the US National Defense University. He offered this definition: ‘A strategy is a plan and iterative process for achieving broad political objectives, that continually takes into account one’s environment, goals, resources, and constraints, as well as those of other interested parties’. Personal communication from G. Miller, 25 August 2017.

67 Tore Bjørgo’s definition: “Strategy is here about putting the available measures and resources into an action plan to achieve a specified effect, e.g., to reduce a specified actor’s capacity to carry out specific actions, such as acts of terrorism. Strategies are therefore based on conceptions of certain mechanisms – a process in which some factors or means influence
the elements and bring about a specific effect. (...) *Measures* are the methods or deliberate courses of action implemented to activate a specific mechanism and through this they achieve an intended effect. (...) It is important to differentiate between a strategy/mechanism and the measures used to activate it. The same measures (e.g., arrest) can trigger different mechanisms (e.g., deterrence, disruption or incapacitation) and this be included in several prevention strategies at the same time, but have a different preventive function in each of these strategies. Similarly, different measures can activate the same mechanisms, e.g., both arrest and exposure in the media can help to disrupt a terror plot.” Bjørgo, Tore *Strategies for Preventing Terrorism*. New York: Palgrave Macmillan, 2013, p. 5.

68 If a strategic plan does, despite its flexibility, not work within a pre-determined period of time, it is important to move to a Plan B. The period of time when Plan A has to be given up and one has to move to a different Plan B should be based on perceived shifts in the balance of power between the opponents as time goes by.


70 UN Plan of Action, point 60.

71 Cf. Tom Parker. *Avoiding the Terrorist Trap. Why Respect for Human Rights is the Key to Defeating Terrorism*. London: World Scientific, 2019. See also Tom Parker’s chapter in this *Handbook* making a strong case in this regard. Parker was also one of the primary drafters of the UN Plan of Action.


74 UN Plan of Action point 44 (a).

75 Ibid., point 45 (a).

76 A/RES/60/288, 8 September 2006. The Plan of Action in the Annex to the resolution covers four areas:

1. Pillar: Measures to address conditions conducive to the spread of terrorism (e.g. A. Countering the appeal of terrorism; B. Preventing and resolving conflicts; C. Fostering Dialogue and understanding; D. Promoting economic and social development);

2. Pillar II: Measures to prevent and combat terrorism (A. Activities on law enforcement and border control; B. Activities on preventing and responding to attacks by means of weapons of mass destruction; C. Activities on combating the financing of terrorism; D. Activities on protecting vulnerable targets, critical infrastructure and the Internet).

3. Pillar III. Measures to build States’ capacity to prevent and combat terrorism and strengthen the role of the United Nations system in this regard (A. Facilitating the integrated implementation of the United Nations Global Counter-Terrorism Strategy; B. Enhancing the capacity of criminal justice officials and law enforcement officers).

4. Pillar IV: Measures to ensure the protection of human rights and the rule of law while combating terrorism (A. Training and capacity-building for law enforcement officials on human rights, the rule of law and the prevention of terrorism; B. Basic human rights reference guides C. Support for victims of terrorism).


78 The absence of “political will” can be linked to an absence of “political insight.” However, sad enough, there is also a more sinister explanation for the lack of political will by some
regimes. Having a “public enemy” whether in the form of one or more enemy “rogue states” abroad or in the form of one or more domestic or foreign terrorist groups, serves some demagogic regimes well. It allows them to “play politics” with the public’s fear of terrorism – a fear that can be manipulated, and one that has in some cases even led to ‘false flag’ operations. This author remembers, while he was on an official UN mission, a sentence from a briefing he received from a local expert: “Not all bombs that explode here are the work of terrorists”.


Bibliography


Neuecker, Christine Helene (2017, Summer): *CVE Programs and Initiatives through the Ages: A Snapshot of the Past, Present, and Future*. (Master’s Thesis, Simon Fraser University, Burnaby, Canada). Available at: http://summit.sfu.ca/item/17537

Neumann, P. (2017): *Countering Violent Extremism and Radicalisation that lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region*. Vienna: OSCE.

NACJD: Resource Guide: Terrorism & Preparedness Data. Available at: https://www.icpsr.umich.edu/icpsrweb/content/NACJD-guides/tpdrc.html


OSCE (2014), Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach. Vienna: OSCE.


RAN YF&C (2017): Strengthening Community Resilience to Polarization & Radicalization. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-

Ranstorp, Magnus; Hyllengren, Peder (2013): Prevention of Violent Extremism in Third Countries: Measures to Prevent Individuals Joining Armed Extremist Groups in Conflict Zones. (CATS Report). Available at: https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives/Perspectives on Terrorism/Abingdon: Routledge, 223


Schoeman, Albertus (2017, September): Will Limits on Free Expression Prevent Terrorism? (ISS Africa in the World Reports, No. 2). Available at:


Zisner, Jeff (2013): *How to prevent a terrorist bombing or terrorist attack*. AEGIS. Available at: http://www.aegis.com/how-to-prevent-a-terrorist-bombing-attack/
Web-based Resources

Bundesamt für politische Bildung. Available at: https://bpb.de/ radikalisierungsprävention
Canadian Practitioners Network for the Prevention of Radicalization and Extremist Violence (CPN-PREV) Université du Québec à Montréal (UQAM). Available at: www.cpnprev.ca.
Extremismuspräventionsatlas.[Atlas for Extremism Prevention] Available at: https://www.handbuch-extremismuspraevention.de/static/HEx/index.html
Mapping Resources on Preventing Violent Extremism. Available at: https://docs.google.com/spreadsheets/d/1gswn_0AHpdRaHuUAs--oKatd558jxvc-5d6RqZzFSOw/htmlview.
ResearchGate. Terrorism Prevention. Available at: https://www.researchgate.net/search/publications?q=Terrorism%2BPrevention
Society for Prevention Research. Available at: https://www.preventionresearch.org/
General Bibliography on Terrorism Prevention and Preparedness

Compiled and Selected by Ishaansh Singh

This bibliography contains bibliographies, books, journal articles, book chapters, theses, edited volumes, grey literature, websites, and other sources which have been organised into five sections:

1. “General Terrorism Prevention (including Prevention of Conflict, Crime, Violence),”
2. “Prevention of Radicalization (including Deradicalization),”
3. “Prevention of Terrorism and (Violent) Extremism,”
4. “Preparedness,” and
5. “Anti- and Counter-Terrorism.”

Each section contains approximately 360 titles.

Keywords: antiterrorism, bibliography, terrorism prevention, radicalization, deradicalization, (violent) extremism, preparedness, programs, counterterrorism.
1. General Terrorism Prevention (Including Prevention of Conflict, Crime, and Violence)

Bibliographies and other Resources


Mapping Resources on Preventing Violent Extremism (n.d.). Available at: https://docs.google.com/spreadsheets/d/1gswn_0AHpdRaHuUAs--oKatd558jxve-5d6RqZzFSOw/htmlview

[US] National Criminal Justice Reference Service. Terrorism Prevention. ADD. Available at: https://www.ojp.gov/ncjrs/virtual-library/search?delta=All&title=Terrorism+Prevention&field_authors_value=&journal_name=&field_ncj_number_value=&pub_date_max=&pub_date_min=&combine_keywords=&sort_by=field_year_published_value&sort_order=DESC


Books and Edited Volumes


Spaaij, Ramón (2012): Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention. (Springer Briefs in Criminology). Dordrecht: Springer. Available at: https://doi.org/10.1007/978-94-007-2981-0


**Theses (Ph.D. & M.A./M.Sc.)**


Block, Molly Mae (2016): *Applying Situational Crime Prevention to Terrorism Against Airports and Aircrafts*. (Ph.D. Thesis (English), University of Louisville). Available at: http://ir.library.louisville.edu/etd/2479


*Articles and Book Chapters (in Edited Volumes)*


Goh, Gillian & Clark, Christopher (2011): How to keep ammunition out of the hands of terrorists. NATO. Available at: https://www.nato.int/docu/review/articles/2011/06/01/how-to-keep-ammunition-out-of-the-hands-of-terrorists/index.html


Gruenewald, Jeff et al. (2019, August): A Situated Comparison of Suicide and Non-Suicide Terrorist Plots and Homicides in the United States, 1990-2014. *Crime & Delinquency*, 65(9), 1187-1217. Available at: https://doi.org/10.1177/0011128718796461


Perry, Simon; Hasisi, Badi; Perry, Gali (2019, January): Lone Terrorists: A Study of Run-Over Attacks in Israel. European Journal of Criminology, 16(1), 102-123. Available at: https://doi.org/10.1177/1477370818769257


Pyszczynski, Tom; Vail, Kenneth E., III; Motyl, Matthew S. (2009): The Cycle of Righteous Killing: Psychological Forces in its Prevention and the Promotion of Peace. In:


Qurashi, Fahid (2018, February): The Prevent Strategy and the UK “War on Terror”: Embedding Infrastructures of Surveillance in Muslim Communities. *Palgrave Communications*, 4, Article 17. Available at: https://doi.org/10.1057/s41599-017-0061-9


Richards, Anthony (2011, January): The Problem with “Radicalization”: The Remit of “Prevent” and the Need to Refocus on Terrorism in the UK. *International Affairs*, 87(1), 143-152. Available at: https://doi.org/10.1111/j.1468-2346.2011.00964.x


Weine, Stevan M. et al. (2017, January): Violent Extremism, Community-Based Violence Prevention, and Mental Health Professionals. *The Journal of Nervous and Mental Disease*, 205(1), 54-57. Available at: https://doi.org/10.1097/NMD.0000000000000634 Available at: https://indigo.uic.edu/handle/10027/21690


**Grey Literature**


Bühler, Anneke/Groeger-Roth; Frederick (2013): Do we need a “Red list prevention”? What is not recommended in prevention? In: Kerner, Hans-Jürgen & Marks, Erich (Publ.): Internet Documentation of the German Congress of Crime Prevention. Hanover, 2013. Available at: www.praeventionstag.de/Dokumentation.cms/2361

Bunn, Matthew et al. (2016, March): Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline? (Report; Belfer Center for Science and International Affairs, Project on Managing the Atom). Available at: https://www.belfercenter.org/publication/preventing-nuclear-terrorism-continuous-improvement-or-dangerous-decline


Cook, Joana (2017): Avoiding the Pitfalls of Prevent. (GIWPS Paper; Bridging Theory & Practice series). Available at: https://giwps.georgetown.edu/resource/avoiding-the-pitfalls-of-prevent


EU Counter-Terrorism Coordinator (2012): Preventing Lone Actor Terrorism - Food for Thought. Available at: https://www.eumonitor.nl/9353000/1/j9vzik7m1c3gyxp/vj6ipob5v8f0


Institute for Policy Analysis of Conflict (IPAC) (2019, January): *Protecting the Sulu-Sulawesi Seas from Abu Sayyaf Attacks.* (IPAC Report No. 53). Available at:


Jones, Michael & Winterbotham, Emily (2020): Research Methodology: The Prevention Project. RUSI. Available at: https://rusi.org/publication/other-publications/prevention-project-methodology


Steffen, Wiebke (2014): *Report for the 19th German Congress of Crime Prevention*. DPT. Available at:
https://www.praeventionstag.de/dokumentation/download.cms?id=2065&date
i=1-Wiebe-StepfenF_2065.pdf


Stuart, Hannah (2014, September): British Jihadists: Preventing Travel Abroad and Stopping
Attacks at Home. (CRT Policy Paper No. 1). Available at:

Sutton, Rupert (2016, September): Myths and Misunderstandings: Understanding Opposition
to the Prevent Strategy. (CRT Policy Paper No. 7). Available at:

The City of Aarhus and East Jutland Police (2015). Building resilience to radicalisation and

UN (2015): Measures to prevent terrorists from acquiring weapons of mass destruction.
Available at: https://gafcvote.un.org/UNODA/vote.nsf/91a5e1195de97a630505b
8adf/38982ec3e13278835257f1b005d3ce8/$FILE/A%20RES%2070%2036.pdf

United Nations Office on Drugs and Crime & United Nations Human Settlements
Assessment Toolkit.

United States Congress et al. (2017): World at Risk: A Report from the Commission on the
Prevention of Weapons of Mass Destruction, Proliferation and Terrorism.

US. Commission on the Prevention of Weapons of Mass Destruction Proliferation and
Terrorism (2009): The Clock is Ticking: a Progress Report on America’s
Preparedness to Prevent Weapons of Mass Destruction Proliferation and
 Destruction Proliferation and Terrorism. Available at:
https://www.centerforhealthsecurity.org/resources/interactives/rad-resilient-
city/references/03WMDRpt10-20Final.pdf

US Government (2017): Terrorism Prevention and Critical Infrastructure Protection Act of
2017.

49.25. Geneva, Switzerland: World Health Organization. Available at:
https://apps.who.int/iris/handle/10665/179463

Wuchte, Thomas (2014): Kidnapping for Ransom - the OSCE as a Regional Approach. UN
Workshop ‘Preventing and responding to terrorist kidnapping and hostage-taking’. Available at:
https://www.osce.org/secretariat/128071

Yang, Sue-Ming; Su, Yi-Yuan; Varriale Carson, Jennifer (2014, May): Eco-Terrorism and
the Corresponding Legislative Efforts to Intervene and Prevent Future Attacks.
(TSAS Working Paper Series, No. 14-04). Available at:
esponding-legislative-efforts-to-intervene-and-prevent-future-attacks

Zisner, Jeff (2013): How to Prevent a Terrorist Bombing or Terrorist Attack. AEGIS.
Available at: http://www.aegis.com/how-to-prevent-a-terrorist-bombing-attack/

Relevant Websites

(US) National Criminal Justice Reference Service: listing ca. 500 items on ‘Terrorism
Prevention’: Available at:
https://www.ncjrs.gov/App/AbstractDB/AbstractDBSearchResults.aspx?Title=&a
2. Prevention of Radicalization (including De-radicalization)

**Bibliographies and other Resources**

Centre for the Prevention of Radicalization Leading to Violence (CPRLV) (2015, March): Available at: https://info-radical.org/en

European Eye on Radicalization (EER) (n.d.): *Radicalization and Deradicalization Bibliography*. Available at: https://ceradicalization.com/bibliographies/#1547464178047-5448dd14-2ca8

German Institute on Radicalization and De-radicalization Studies (GIRDS) (2014): Available at: http://girds.org


Kompetenznetzwerk Radikalisierungsprävention (2017-). Available at: https://www.netzwerk-deradikalisierung.com

Middle East Institute (MEI); Fondation pour la Recherche Stratégique (FRS) (eds.) (2015, June): *Understanding Deradicalization: Pathways to Enhance Transatlantic Common Perceptions and Practices*. [Essay Collection]. Available at: https://www.mei.edu/publications/understanding-deradicalization-pathways-enhance-transatlantic-common-perceptions-and


Wagner, Bernd (ed.-in-Chief) (2013-): Journal EXIT-Deutschland (JEX): Journal for Deradicalization and Democratic Culture. ISSN: 2196-8136. Available at: http://journals.sfu.ca/jed

Books and Edited Volumes


Theses (Ph.D. & M.A./M.Sci.)


Ndili, Alex (2016, November): The Role of Community Policing in the Prevention of Youth Radicalization in the Eastleigh Area of Nairobi County. (Master’s Thesis, University of Nairobi, Nairobi, Kenya). Available at: http://hdl.handle.net/11295/100166


### Articles and Book Chapters (in Edited Volumes)


Cherney, Adrian (2016): Designing and Implementing Programmes to Tackle Radicalization and Violent Extremism: Lessons from Criminology. *Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide*, 9(1-3), 82-94. Available at: https://doi.org/10.1080/17467586.2016.1267865


Mythen, Gabe; Walklate, Sandra; Peatfield, Elizabeth-Jane (2017, May): Assembling and Deconstructing Radicalisation in PREVENT: A Case of Policy-Based Evidence


Sian, Katy (2017, October): Born Radicals? Prevent, Positivism, and “Race-Thinking”. *Palgrave Communications*, 3, Article 6. Available at: https://doi.org/10.1057/s41599-017-0009-0


Grey Literature


Davies, Matthew; Warnes, Richard; Hofman, Joanna (2017): *Exploring the Transferability and Applicability of Gang Evaluation Methodologies to Counter-Violent Radicalisation*. (RAND Research Reports, RR-2120-EC). Available at: https://doi.org/10.7249/RR2120


https://www.belfercenter.org/publication/beyond-cve-evolving-us-countering-violent-extremism-policy-prevent-growing-threat


Hedayah; Centre for Analysis of the Radical Right (CARR) (2020, November): Radical Right Counter Narratives. (Expert Workshop Report). Available at: https://www.hedayahcenter.org/resources/reports_and_publications/radical-right-counter-narratives-expert-workshop-report


**Relevant Websites**


3. Prevention of Terrorism and (Violent) Extremism

**Bibliographies and other Resources**


Kompetenzzentrum gegen Extremismus in Baden-Württemberg (konex) (2015): Available at: https://www.konex-bw.de


Winterbotham, Emily (2020): The Prevention Project: Introduction to the Publication Series. RUSI. Available at: https://rusi.org/publication/other-publications/prevention-project-introduction-publication-series

**Books and Edited Volumes**


**Theses (Ph.D. & M.A./M.Sc.)**


Neudecker, Christine Helene (2017, Summer): *CVE Programs and Initiatives through the Ages: A Snapshot of the Past, Present, and Future.* (Master’s Thesis, Simon Fraser University, Burnaby, Canada). Available at: http://summit.sfu.ca/item/17537


Articles and Book Chapters (in Edited Volumes)


Fitzgerald, James (2016): Frontline Perspectives on Preventing Violent Extremism: An Interview with Alyas Karmani (STREET UK). *Critical Studies on Terrorism*, 9(1), 139-149. Available at: https://doi.org/10.1080/17539153.2016.1147769


Ganesh, Bharath; Bright, Jonathan (2020): Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation. *Policy & Internet*, 12(1), 6-19. Available at: https://onlinelibrary.wiley.com/toc/19442866/2020/12/1


Global Center on Cooperative Society (2020): *Enhancing Civil Society Engagement*. Available at: https://www.globalcenter.org/publications/enhancing-civil-society-engagement


Lombardi, Marco; Lucini, Barbara; Maiolino, Marco (2020): New Perspectives in Preventing and Countering Violent Extremism. Security Terrorism Society, 11. Available at: https://www sicurezzaterrorismosocieta.it/fascicolo-11-2020/


Handbooks in Criminology and Criminal Justice). Chichester: John Wiley & Sons, 449-467. Available at: https://doi.org/10.1002/9781118923986.ch29


Wilner, Alex; Rigato, Brandon, on behalf of the “60 Days of PVE” Group (2017): The 60 Days of PVE Campaign: Lessons on Organizing an Online, Peer-to-Peer, Counter-Radicalization Program. *Journal for Deradicalization*, 12, 227-268. Available at: http://journals.sfu.ca/jd/index.php/jd/article/view/117


**Grey Literature**


Available at: https://www.isdglobal.org/isd-publications/gifct-countering-violent-extremism-toolkit


Krasenberg, Jordy; Gssime, Yasmine (2019, May): Taking Mental Health Insights into Account in Local P/CVE. (RAN Ex Post Paper). Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-


Millar, Alistair (2017, May): Updated Guidance on ODA-Eligible Activities for Preventing Violent Extremism: Implications and Opportunities for the European Union. (CT-
SINGH 1217


Radicalisation Awareness Network (RAN) (2020, January): *The Role of Restorative Justice in Preventing and Responding to Violent Extremism.* Available at:

Ranstorp, Magnus; Hyllengren, Peder (2013): *Prevention of Violent Extremism in Third Countries: Measures to Prevent Individuals Joining Armed Extremist Groups in Conflict Zones.* (CATS Report). Available at:
http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-4449


Saltman, Erin Marie; Kirt, Jas (2016, June): *Guidance for International Youth Engagement in PVE and CVE: Youth Responses to Resolution 2250 and the UN Plan of Action to Prevent Violent Extremism.* (ISD / YouthCAN Report). Available at:


Schanzer, David; Eyerman, Joe (2019, August): *Engaging with Communities to Prevent Violent Extremism: A Review of the Obama Administration’s CVE Initiative.* (Triangle Center on Terrorism and Homeland Security / RTI International Report). Available at: https://sites.duke.edu/tcths/2019/08/14/new-report-outlines-key-flaws-with-obama-administrations-countering-violent-extremism-initiative

Schwartz, Matthew (2018, September): *Shifting the PVE Paradigm: A Think Piece on Human Insecurity, Political Violence, and New Directions for Preventing Violent Extremism.* (Global Center on Cooperative Security Policy Brief). Available at:
https://www.globalcenter.org/publications/shifting-the-pve-paradigm

Sharland, Lisa (2017, November): *Preventing and Countering Violent Extremism in Africa: Mining and Australia’s Interests.* (ASPI Strategic Insights, No. 124). Available at:


Relevant Websites


Kofi Annan (2017): Extremely together. Available at: http://www.extremelytogethertheguide.org/?mc_cid=186efc97f2&mc_eid=87b2997a0a

MASAR. Available at: hedayahcenter.org/resources/interactive_cve_apps/masar/

START News: How to Build Programs to Prevent Violent Extremism; START-Oxford collaboration launches first book; Free, online CVE course, Available at: https://mailchi.mp/start/q86rfojms6-357989?e=bb5496e80f

The Week (June 30, 2019): G20 Leaders Resolve to Prevent Use of Internet for Terrorism, Extremism. Available at: https://www.theweek.in/news/world/2019/06/30/g20-leaders-resolve-to-prevent-use-of-internet-for-terrorism-extremism.html
4. Preparedness (including Resilience and Crisis Management)

**Bibliographies and other Resources**


Terrorism & Preparedness Data Resource Center (TPDRC) (n.d.-): Available at: https://www.icpsr.umich.edu/icpsrweb/content/NACJD/guides/tpdrc.html

Texas Health and Human Services (n.d.): *Bioterrorism-Disaster Preparedness Resources*. Available at: https://www.dshs.state.tx.us/library/bt-books.shtm


United States Department of Labour: *Emergency Preparedness and Response - Chemical Terrorism*. Available at: https://www.osha.gov/SLTC/emergencypreparedness/chemical_sub.html

**Books and Edited Volumes**


Chen, Thomas M., Jarvis, Lee & Macdonald, Stuart (2014): *Cyberterrorism: Understanding, Assessment, and Response*. Springer. Available at: https://books.google.es/books?id=IInkAwAAQBAJ&pg=PA8&lpg=PA8&dq=preventing+cyber-terrorism&source=bl&ots=77WF1wB3we&sig=MIJYr-cqY8lG5i9oxpsW5lbZH1o&hl=en&sa=X&ved=0ahUKEwirg4q0u8XTAhWMPBQKHRP5CMA4ChDoAQhlMA0#v=onepage&q=preventing%20cyber-terrorism&f=false


Keyes, Daniel C. et al. (2004): Medical Response to Terrorism: Preparedness and Clinical Practice (2nd ed.). LWW. Available at: https://www.amazon.com/Medical-Response-Terrorism-Preparedness-Clinical/dp/0781749867


Miah, Shamim (2017): Muslims, Schooling and Security: Trojan Horse, Prevent and Racial Politics. Cham: Palgrave Macmillan / Springer Nature. Available at: https://doi.org/10.1007/978-3-319-52335-4


OSCE (2008): Guidebook on Democratic Policing by the Senior Police Adviser to the OSCE Secretary General. “Summary by the Representative of the OSCE Chairman-in-Office”. (SPMU Publication Series Vol. 1, 2nd ed.). Vienna. OSCE,


Vaseashta, Ashok; Braman, Eric; Susmann, Philip (eds.) (2012): Technological Innovations in Sensing and Detection of Chemical, Biological, Radiological, Nuclear Threats and Ecological Terrorism. (NATO Science for Peace and Security Series – A: Chemistry and Biology). Dordrecht: Springer. Available at: https://doi.org/10.1007/978-94-007-2488-4

Walter L. Perry et al. (2013): Predicting Suicide Attacks Integrating Spatial, Temporal, and Social Features of Terrorist Attack Targets. St. Monica: RAND. Available at:
http://www.rand.org/content/dam/rand/pubs/monographs/MG1200/MG1246/RAND_MG1246.pdf


**Theses (Ph.D. & M.A./M.Sci.)**


Comens, Cayla (2016): Terrorism Preparedness: A Law Enforcement Perspective. (Master’s Thesis, Department of Criminal Justice Sciences, Illinois State University). Available at: https://ir.library.illinoisstate.edu/cgi/viewcontent.cgi?article=1490&amp;context=etd


Groves, Season (2013): *Knowledge, Involvement and Emergency Preparedness*. (Master’s Thesis, College of Arts and Sciences, University of South Florida). Available at: https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=5880&amp;context=etd


Articles and Book Chapters (in Edited Volumes)

Ackerman, G. et al. (2007): Assessing Terrorist Motivations for Attacking Critical Infrastructure. Lawrence Livermore National Laboratory.


Apostolakis, George E. & Lemon, Douglas M. (2005): A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. Risk


Clemmow, Caitlin; Schumann, Sandy; Salman, Nadine L.; Gill, Paul (2020): The Base Rate Study: Developing Base Rates for Risk Factors and Indicators for Engagement in Violent Extremism. *Journal of Forensic Sciences*, 65(3), 865-881. Available at: https://doi.org/10.1111/1556-4029.14282


Manning, Frederick J. & Goldfrank, Lewis (eds.) (2002): Preparing for Terrorism: Tools for Evaluating the Metropolitan Medical Response System Program. Available at: https://www.nap.edu/read/10412/chapter/8


National Center for Injury Prevention and Control (2010): *Interim planning guidance for preparedness and response to a mass casualty event resulting from terrorist use of explosives*. Atlanta, GA: Center for Disease Control and Prevention. Available at:


Prenzler, Tim; Manning, Matt; Bates, Lyndel (2015): The Implications of a Harm Perspective on Terrorism, Road Safety, Tobacco, Alcohol, Illicit Drugs and Workplace Health and Safety. *Journal of Policing, Intelligence and Counter Terrorism*, 10(2), 88-101. Available at: https://doi.org/10.1080/18335330.2015.1090050


Su, Yi-Yuan; Yang, Sue-Ming (2017): Legislative Efforts to Prevent Eco-Terrorist Attacks. In: Gary LaFree; Joshua D. Freilich (eds.): *The Handbook of the Criminology of Terrorism*. (Wiley Handbooks in Criminology and Criminal Justice). Chichester:
John Wiley & Sons, 535-552. Available at: https://doi.org/10.1002/9781118923986.ch35


Walker, Clive; Conway, Maura (2015): Online Terrorism and Online Laws. *Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide*, 8(2), 156-175. Available at: https://doi.org/10.1080/17467586.2015.1065078


Grey Literature


Boutin, Bérénice (2016, December): Administrative Measures against Foreign Fighters: In Search of Limits and Safeguards. (ICCT Research Paper). Available at: https://doi.org/10.19165/2016.1.15


MMWR (2000): Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response. Available at: https://www.cdc.gov/mmwr/preview/mmwrhtml/rr4904a1.htm


**Relevant Websites**


American Hospital Association: *Emergency Readiness.* Available at: https://www.aha.org/websites/2006-05-12-emergency-readiness

American Red Cross: *Terrorism Safety Tips.* Available at: https://www.redcross.org/get-help/how-to-prepare-for-emergencies/types-of-emergencies/terrorism.html

Ammo.com: *How to Survive a Terrorist Attack: Prepare, Plan, and Survive.* Available at: https://ammo.com/articles/terrorism-disaster-preparedness

Campus Safety. Available at: https://www.campussafetymagazine.com/safety/10_critical_protocols_for_enhanced_school-terrorism_preparedness/

Centre for Disease Control and Prevention: *CDC’s Terrorism Preparedness and Emergency Response Effort.* Available at: https://www.cdc.gov/employment/pdf/COTPER_Overview_Divisions.pdf
Centre for Disease Control and Prevention: *Terrorism Preparedness Compendium*. Morbidity and Mortality Weekly Report. Available at:
https://www.cdc.gov/mmwr/indexbt.html


Department of Labour and Industry: *Dealing with Terrorism*. Available at:

Emergency Preparedness: *Terrorism*. Available at:
https://www.calhospitalprepare.org/terrorism

Google Scholar: *Terrorism Preparedness*. Available at:
https://scholar.google.at/scholar?hl=en&as_sdt=0%2C5&q=Terrorism+Preparedness+&btnG


Metropolitan Police: *Staying Safe from Terrorism*. Available at:

NACJD: *Resource Guide: Terrorism & Preparedness Data*. Available at:
https://www.icpsr.umich.edu/icpsrweb/content/NACJD/guides/tpdrc.html

New York State, Department of Health: *Chemical Terrorism Preparedness and Response Card*. Available at:
https://www.health.ny.gov/environmental/emergency/chemical_terrorism/chemical.htm

North Dakota Department of Health: *Be Aware and be Prepared: An Emergency and Terrorism Preparedness Guide for North Dakotans*. Available at:
https://www.health.nd.gov/media/1091/bioterrorpreparednessguide.pdf

Psychology Today: *10 Ways to Protect Yourself in a Terrorist Attack*. Available at:

Public Health Emergency: *Responders, Clinicians & Practitioners*. Available at:

RAND Corporation: *When It Comes to Terrorism, How Prepared Are Local and State Agencies?* Available at: https://www.rand.org/pubs/research_briefs/RB9209.html

ReadyAtlantic.org: *Preparing for a Terrorist Attack*. Available at:
https://readyatlantic.org/prepare/homesec-preplan.asp

Ready Illinois: *Terrorism*. Available at:
https://www2.illinois.gov/ready/hazards/Pages/Terrorism.aspx

Safety.com: *Keeping Your Family Safe During a Terrorist Attack*. Available at:

Securitas: *Security and Safety Awareness Tips*. Available at:

Southern Nevada Health District: *Preparing for a Terrorist Bombing: A Common Sense Approach*. Available at:
https://www.southernnevadahealthdistrict.org/programs/emergency-preparedness/preparing-for-a-terrorist-bombing-a-common-sense-approach/


TRIP (Travel Responsibly, Informed and Protected): *Precautions to Avoid Being the Target of a Terrorist Attack*. Available at: http://trip.ustia.org/security/tips/1190/precautions-to-avoid-being-being-the-target-of-a-terrorist-attack/

6. Anti- and Counter-Terrorism: General

**Bibliographies and other Resources**


**Books and Edited Volumes**


Organization for Security and Co-operation in Europe (OSCE), Transnational Threats Department (TNTD), Action against Terrorism Unit (ATU) (2019, May): Understanding the Role of Gender in Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism: Good Practices for Law


---

**Theses (Ph.D. & M.A./M. Sci.)**


**Articles and Book Chapters (in Edited Volumes)**


Glazzard, Andrew; Reed, Alastair (2020): Beyond Prevention: The Role of Strategic Communications Across the Four Pillars of Counterterrorism Strategy. *The RUSI
Journal, 165(1), 74-88. Available at: https://doi.org/10.1080/03071847.2020.1727165


Keatinge, Tom; Keen, Florence (2019): Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool. Studies in Conflict & Terrorism, 42(1-2), 178-205. Available at: https://doi.org/10.1080/1057610X.2018.1513698


Lombardo, Nicholas et al. (2009): A next-generation countermeasure architecture to prevent explosives attacks at large public events. IEEE. Available at: http://ieeexplore.ieee.org/abstract/document/5168043/


Neumann, P. (2017): Countering Violent Extremism and Radicalisation that lead to Terrorism: Ideas, Recommendations, and Good Practices from the OSCE Region. Vienna: OSCE.


Striegler, Jason-Leigh (2013): Early Detection of the Lone Wolf: Advancement of Counter-Terrorism Investigations with an Absence or Abundance of Information and Intelligence. *Journal of Policing, Intelligence and Counter Terrorism, 8*(1), 35-53. Available at: https://doi.org/10.1080/18335330.2013.789596


Williams, Michael J. et al. (2019): Experimental Effects of a Call-Center Disclaimer Regarding Confidentiality on Callers’ Willingness to Make Disclosures Related to Terrorism. *Terrorism and Political Violence, 31*(6), 1327-1341. Available at: https://doi.org/10.1080/09546553.2018.1476347


**Grey Literature**


Guittard, Alexander (2019, September): Counterterrorism is a Public Function: Resetting the Balance between Public and Private Sectors in Preventing Terrorist Use of the Internet. (GW Program on Extremism Paper; Legal Perspectives on Tech Series). Available at: https://extremism.gwu.edu/sites/g/files/zaxdzes2191/f/Counterterrorism%20is%20a%20Public%20Function.pdf


United Nations Human Rights Council (2020): Special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2020) Human rights impact of policies and practices aimed at preventing and


Relevant Websites

Australian National Security: Media and Publications. Available at:

Dag Hammarskjöld Library (n.d.): Counter-Terrorism: Quick Guide. Available at:

Government of the Netherlands: Counterterrorism and National Security. Available at:

Homeland Security and Emergency Services: Counter Terrorism. Available at:
http://www.dhsses.ny.gov/oct/safeguardny/


OSCE (2020): Counter-Terrorism Network Newsletter No. 134. Available at:
https://mailchi.mp/a7be7331a7db/osce-counter-terrorism-network-ctn-newsletter-no-4890858?e=e2c7e7c81e


U.S. Food and Drug Administration: Counterterrorism and Emerging Threats. Available at:


Ishaansh Singh is studying at the Symbiosis School for Liberal Arts, Pune, since 2018. His major and minor fields of specialisation are International Relations and Peace and Conflict Studies. Additionally, he serves as an intern for the Terrorism Research Initiative, Vienna. He is also working on his thesis on the factors that led to Brexit. E-mail: s.ishaansh@gmail.com

Acknowledgement

The compiler of this bibliography would like to thank Judith Tinnes (Leibniz Institute for Psychology Trier), Alex Schmid (ICCT, The Hague) Nina Käsehage (University of Rostock) as well as Alberto Caballero Diez (TRI Spain) for generously sharing their own bibliographies on the prevention of radicalization, extremism and terrorism.
Abu Ghraib Detention Facility, 374
Abu Musab al-Zarqawi, 117, 418, 535, 565, 848
Abu Sayyaf, 119, 170, 361, 514, 515, 1014, 1177
Acceptance, 1250
Accountability, 493, 952, 961, 1136
Adaptation, 254, 949, 955, 959
Adiyaman, Turkey, 410
Advanced Persistent Threat, 876
Advisories, 625, 626, 632
African National Congress, 82
African Union, 16, 168, 516, 843, 846
Agenda Setting, 572
Airport Security, 1024
AK-47, 510, 513, 517, 518
Al Aqsa Intifada, 933, 937, 950
Aldrich, Daniel P., 974, 980, 981
Alerts, 625, 626, 638
Alex Station, 631, 634
al-Hayat Media, 360
Al-Qaeda and Taliban Sanctions Committee 1267, 518
al-Qaeda in the Arabian Peninsula, 360, 362, 512, 621, 666, 1198
Al-Qaeda in the Malay Archipelago, 985, 1003
Alternative Narratives, 1194
American Society for Industrial Security (ASIS), 636, 663, 676
American Terrorism Study, 60, 707
American University in Beirut (AUB), 244, 245
Amri, Anis, 249, 252
Analysis, 9, 223, 257, 274, 378, 413, 456, 493, 574, 629, 636, 676, 882, 980, 983, 1012, 1013, 1018, 1019, 1025, 1026, 1049, 1052, 1054, 1056, 1103, 1149, 1153, 1160, 1162, 1165, 1166, 1167, 1169, 1176, 1177, 1178, 1186, 1188, 1189, 1197, 1200, 1211, 1215, 1219, 1223, 1227, 1229, 1231, 1232, 1234, 1235, 1236, 1239, 1248, 1249, 1251, 1253, 1258
Anger, 142, 143, 147, 148, 154, 210, 211, 220, 230, 254, 297, 430, 667, 670, 936, 966, 998, 1028, 1030, 1035, 1041
Anglo-Irish Treaty, 81
Ankara, Turkey, 174, 246, 247, 251, 403, 410, 427, 478, 1174, 1256
Anonymous, 220, 318, 370, 603, 874, 1033, 1034, 1041, 1049, 1050, 1053, 1057, 1195, 1259
Anonymous Collective, 370
Anti-Terrorism, 1160, 1211, 1228, 1246, 1256, 1258
Antiterrorism Task Force (ATTF), 636
Anwar al-Awlaki, 362, 375, 654, 666, 671
Anxiety, 936, 954, 960, 962, 1174, 1252
Army Public School, 168, 169, 281, 282, 1127
Arson, 7, 678, 687, 688
Artificial Intelligence, 366, 880, 1179
Ask.fm, 368
Asylum Centres, 4, 238
Asylum Seekers, 1236
asymmetric conflict, 139, 148, 149, 154, 155, 156, 1106
Attractiveness, 1169
Attrition, 119, 130
Aum Shinrikyo, 535, 539, 544, 625, 802, 967
Average Mohammad, 374
aviation, 628, 632, 708, 790, 791, 792, 793, 794, 795, 796, 799, 800, 803, 806, 807, 808, 809, 839, 849, 854, 858, 890, 898, 964
Azov Battalion, 514
Bad news, 571
Baghdad, 121, 231, 621, 711, 715
Baghdadi, al-, Abu Bakr, 113, 120, 125, 182, 361, 405
Bali, 9, 360, 985, 986, 988-1009, 1012-1017, 1019, 1021-1025
Balochistan, 272
Ban Ki-Moon, 1117
Bangladesh, 246, 480, 513, 671, 877, 1206, 1216
Barriers, 1018, 1026, 1167, 1192, 1199, 1212
Behavioral detection, 709, 807
Beirut International Airport, 710
Belfast, 545, 688, 711, 715
Benevolent Radicalization, 27
Berger, J.M., 1152
Berger, Rony, 937, 954, 960
Best Practices, 225, 979, 984, 1191, 1200, 1211, 1212
Bjørgo, Tore, 23, 30, 50, 51, 53, 63, 64, 1032, 1033, 1039, 1042, 1043, 1044, 1049, 1050, 1051, 1052, 1053, 1054, 1055, 1119, 1145, 1149, 1152, 1155, 1161, 1173, 1176, 1244, 1249
Black Hand, 572
Black September Organization, 629
Blocking Content, 368
Bloody Friday, 711
Bloody Sunday, 152
Bojinka plot, 794, 795
Boko Haram, 168, 173, 479, 513, 515, 516, 733, 737, 768, 1036, 1037, 1040, 1041, 1046, 1050, 1051, 1056, 1124, 1126, 1127, 1146, 1178, 1207, 1222
Bolhuis, Maarten P., 1236
Borders, 177, 182, 475, 478, 480, 482, 494, 495, 1019, 1025, 1231, 1248
Bosnia-Herzegovina, 82, 86, 477, 749, 1192, 1211, 1219
Brand, 1193, 1255
Breivik, Anders Behring, 111, 685, 686, 1045, 1127
Brom, Danny, 933, 952, 953, 957, 958, 959, 960, 961
Brookings Institution, 244, 1052, 1054, 1245
Bulletins, 632, 637, 638
Burav Avenger, 372
Bush, George W., 76, 81, 124, 125, 445, 449, 476, 491, 493, 627, 997, 1245, 1252
Caliphate, 116, 120, 128, 873, 874, 1168, 1170, 1174
Campaigns, 9, 374, 802, 1027, 1196
Canada, 224, 373, 409, 447, 448, 456, 457, 459, 482, 491, 601, 633, 640, 741, 882, 951, 1035, 1050, 1053, 1153, 1176, 1188, 1191, 1199, 1204, 1223, 1226, 1227, 1233
Capability, 312, 612, 747, 887
Carter, Jimmy, 573, 629, 1202, 1244
Cato Institute, 240
Causes of Terrorism, 35, 1050, 1052, 1053, 1054, 1145, 1155, 1168, 1173, 1244
CCTV, 60, 61, 611, 685, 706, 709, 711, 714, 715, 807, 818, 854, 857, 858, 890, 1007
Cell, 453, 676
Censorship, 580
Center for Strategic Counter-Terrorism Communications (CSCC), 374
Central Intelligence Agency (CIA), 510
European Parliament, xxv, 177, 368, 565, 1147, 1148, 1195, 1196
European Union, 5, 16, 26, 248, 317, 474, 495, 520, 678, 828, 1117, 1121, 1177, 1187, 1195, 1198, 1213, 1216, 1253, 1257
EVIL DONE, 56, 59, 60, 62, 706, 707
Execution, 599, 600, 748, 824
Executive Order 12977, 713
Explosives, 508, 509, 510, 511, 516, 518, 535, 685, 793, 807, 848, 1234, 1247, 1248
Exposed, 56, 59, 707, 953, 954, 956, 958, 959
Family, 308, 312, 318, 415, 942, 949, 957, 959, 977, 981, 1050, 1143, 1152, 1187, 1191, 1201, 1206, 1242
FARC, 89, 510, 514, 515, 737
Fatah, 127, 769, 772, 774, 775, 777, 779
Federal Emergency Management Agency (FEMA), 636, 897, 969
Federally Administered Tribal Areas, 282
Financial Intelligence, 455
Financial Intelligence Units (FIUs), 455
Financing, 444, 445, 446, 449, 451, 452, 453, 454, 457, 598, 600, 1164, 1167, 1208, 1245, 1252, 1256
Firearms, 509, 681, 848, 1176, 1233
First Responders, 940, 942, 955, 958, 959, 1166
Flickr, 364, 599
Followers, 422
Forecasting, 145, 844, 1018, 1021, 1224
Foreign Terrorist Fighter (FTF), 478, 484, 601, 1239
Frank, Michael C., 952, 958
Free Syrian Army (FSA), 244, 246
Front de Libération Nationale, 81, 1030
FRONTEX, 474
Fuerzas Armadas Revolucionarias de Colombia — Ejército del Pueblo (FARC-EP), 89, 510, 514, 515, 737
Fundamentalism, 1244
Funding, 247, 278, 282
Gaza Strip, 447, 773, 774, 776, 777, 778
Genocide, 3, 24, 63, 139, 140, 141, 142, 144, 145, 156, 240, 1036, 1127
Germany, 4, 92, 128, 145, 149, 150, 152, 167, 208, 247, 250, 251, 252, 253, 291, 293, 294, 301, 307, 308, 309, 310, 319, 320, 370, 456, 487, 535,
538, 567, 572, 613, 627, 629, 630, 641, 682, 687, 688, 802, 877, 971, 991, 1144, 1189, 1192, 1196, 1199, 1202, 1203, 1207
Global Center on Cooperative Security, 1118, 1143, 1148, 1149, 1152, 1177, 1179, 1206, 1212, 1213, 1214, 1216, 1217, 1218, 1240, 1241
Global Compact on Refugees, 246
Global Counter Terrorism Forum, 8, 378, 828, 839, 1214
Global Counterterrorism Forum (GCTF, 378, 1214
Global Engagement Center, 374
Global Internet Forum to Counter Terrorism (GIFCT), 367, 370
Global Strategy, 1116, 1125
Global Terrorism Database, 511, 679, 708, 842, 986, 1111
Global Terrorism Index, 705, 823, 1112, 1145
Global War on Terror (see also War on Terror), 2, 271, 279, 985, 987, 991, 997, 1006, 1007, 1017, 1046, 1104, 1123, 1244, 1255
Google, 20, 152, 244, 368, 376, 595, 596, 610, 611, 1216, 1242
Gordon, Jr., R.S., 20, 875, 1002, 1003, 1012, 1013, 1014, 1015, 1016, 1017, 1018, 1019, 1020, 1021, 1022, 1023, 1024, 1025, 1026, 1167, 1187, 1200, 1206, 1231, 1236, 1238
Gough, Ian, 14, 21
Governance, 8, 28, 129, 860, 892, 1107, 1145, 1205, 1207, 1214, 1231, 1232, 1247
Great Britain, 4, 110, 117, 208
Greece, 5, 6, 244, 247, 303, 308, 477, 488, 489, 547, 613
Grenades, 510
Guantanamo, 230, 374, 1235
Gulf Cooperation Council, 272
Gurr, Ted R., 17, 140, 141, 1162, 1223
Guterres, António, 296, 880, 1105, 1117
Hacking, 540, 874
Hague Convention, 793, 850
Hamas, 81, 87, 88, 117, 126, 127, 493, 510, 511, 512, 513, 515, 517, 768, 769, 773, 774, 776, 779
Hamiel, Daniel, 956, 958
Haqqani network, 81
Harakat ut Taleem, 374
Hate Speech, 946
Haugen, Peter T., 955, 958
Hedayah, the International Center of Excellence for Countering Violent Extremism, 378, 379
Hezbollah, 78, 81, 87, 127, 398, 404, 415, 427, 446, 447, 512, 515, 517, 604, 625, 626, 627, 629, 635, 640, 707, 767, 768, 769, 772, 778, 873
Hijacking, 7, 36, 374, 400, 629, 634, 639, 747, 778, 791, 792, 793, 795, 796, 797, 849, 966, 1044
Hillyard, Paddy, 1203
Hirschfeld, Yair, 82
Hobfoll, Stevan, 955, 958
Holbrooke, Richard, 82
Holocaust, 666, 933, 938, 950, 1167
Home Office, 311, 312, 313, 714, 1163, 1177
Homeland Security, 634, 970, 978, 982, 984, 1158, 1225, 1238
Horgan, John, 1220, 1256
Hostage, 7, 732, 734, 736, 737, 738, 742, 743, 744, 749, 1167, 1175
Hostage Taking, 734, 1175
Housing, 213, 214, 250
Hutus, 146, 242
Islamic Revolutionary Guards Corps (IRGC), 512
Islamic State in Iraq and the Levant (ISIL), 453, 455, 516, 898, 1124, 1126, 1127, 1150, 1179, 1189
Islamic State in the Greater Sahara (ISGS), 479
Islamist extremism, 24, 60, 139, 152, 309, 670, 990
Islamophobia, 290, 292, 293, 294, 298, 303, 309
Italy, 111, 150, 152, 208, 249, 303, 484, 489, 547, 629, 630, 634, 802, 805, 1034, 1050
Ittehad-e-Tanzeem-ul-Madaris Pakistan, 272
Jihad, 230, 276, 320, 407, 493, 511, 512, 517, 537, 569, 768, 932, 989, 997, 1001, 1003
Jihadist, 320, 413, 428, 492, 516, 537, 688, 803, 806, 820, 993, 1012, 1022, 1049, 1053, 1056, 1155, 1169, 1172, 1180, 1183, 1184, 1190, 1195, 1196, 1197, 1236, 1254-1256
Jordan, 112, 117, 224, 241, 242, 243, 244, 245, 246, 247, 248, 250, 419, 483, 668, 792, 851, 1144, 1188, 1209
Journalism, 577, 1047, 1057
Jujitsu politics, 154, 155
Junaid Hussain, 874
Justice, 28, 60, 64, 210, 225, 254, 299, 306, 630, 631, 632, 633, 663, 690, 713, 877, 975, 976, 1048, 1050, 1051, 1054, 1055, 1056, 1058, 1107, 1140, 1157, 1160, 1162, 1165, 1169, 1171, 1173, 1175, 1180, 1191, 1197, 1199, 1207, 1211, 1212, 1217, 1218, 1220, 1222, 1226, 1229, 1230, 1231, 1233, 1234, 1235, 1236, 1237, 1241, 1246, 1250, 1253, 1255, 1256
Justpaste.it, 364
Kabar Dunia Islam, 363
Kakuma, 244
Katibat Ansar al Sharia, 361
Kenya, 81, 168, 243, 244, 246, 247, 363, 371, 513, 798, 845, 846, 852, 854, 858, 860, 932, 1029, 1047, 1054, 1127, 1185, 1187, 1193, 1205, 1209
Khyber Pakhtunkhwa, 282
Kidnapping, 733, 734, 746, 747, 748, 848, 1052, 1056, 1168, 1175, 1177, 1180, 1234
Migration, 244, 308, 486, 487, 493, 1186, 1209, 1218, 1229, 1233, 1239, 1249, 1250
Mineta Transportation Institute, 8, 804, 808, 810, 984
Ministry of Religious Affairs, 276, 282
Mishal, Shaul, 1170
Montreal Convention, 793, 850, 853
Moria Camp, 247
Moro Islamic Liberation Front (MILF), 88, 993
Movement for the Emancipation of the Niger Delta (MEND), 847
Mudd, Philip, 1253
- Muslim community, 273, 318, 1041
- Muslim diaspora, 290, 291, 293, 294, 295, 296, 312, 314
Nahdlatul Ulama (NU), 373
Nairobi, 247, 738, 932, 933, 952, 959, 961, 1032, 1185
Narratives, 371, 375, 1019, 1124, 1170, 1183, 1185, 1188, 1192, 1193, 1194, 1195, 1196, 1197, 1200, 1205, 1216, 1220, 1246
National Action Plan, 175, 276, 281, 282, 301, 379, 1152, 1177, 1183, 1214
National Counter Terrorism Authority, 276
National Counter Terrorism Center, 15, 252, 636, 637, 639, 1238
National Counter Terrorism Security Office (NaCTSO), 714, 1248
National Internal Security Policy, 279, 281
National Terrorism Advisory System (NTAS), 638
NATO, 86, 111, 119, 124, 129, 130, 147, 378, 487, 488, 495, 612, 621, 874, 885, 887, 888, 1020, 1104, 1145, 1155, 1161, 1163, 1164, 1167, 1168, 1169, 1171, 1173, 1179, 1184, 1187, 1191, 1192, 1204, 1207, 1210, 1222, 1223, 1225, 1231, 1232, 1236, 1237, 1245, 1246, 1254, 1256
Naxalites, 517, 518
Nazi, 140, 143-145, 149, 167, 308, 371, 568, 569, 655, 659, 667, 670, 672, 673, 685, 688, 821, 822, 1036, 1061, 1064
Negotiation, 86, 741
Netherlands, 31, 117, 128, 129, 224, 249, 250, 254, 255, 297, 303, 546, 547, 578, 746, 830, 980, 982, 1123, 1161, 1185, 1201, 1208, 1228, 1236, 1256, 1259
New People’s Army (NPA), 517
Newman, Graeme, 22, 50, 51, 54, 55, 56, 57, 58, 59, 60, 62, 705, 706, 707, 1016, 1022, 1162, 1168, 1175, 1217, 1223
Nigeria, 112, 113, 168, 173, 224, 479, 513, 515, 542, 733, 737, 768, 847, 1036, 1037, 1040, 1041, 1127, 1178, 1256, 1258
Non-governmental Organizations
(NGOs), 117, 119, 245, 246, 255, 309, 428, 430, 600, 610, 825
Norris, Fran H., 979, 982
North Korea, 452, 512, 517, 535, 536, 542, 546, 640, 794, 877, 878, 895, 896, 898
Northern Ireland, 87, 88, 112, 118, 310, 510, 515, 519, 575, 739, 800, 1038, 1048, 1051, 1055, 1056, 1162, 1170, 1235, 1241
Norway, 111, 249, 293, 294, 299, 308, 457, 768, 1013, 1019, 1035, 1050, 1052, 1053, 1127, 1166, 1207, 1227, 1233
Obama, Barack H., 476, 882, 895, 896, 1105, 1115, 1117, 1147, 1218, 1245
Oklahoma Bombing, 711
Online monitoring, 689
Online payment, 598, 600, 609
Operation Defensive Shield (ODS), 778
Orange Volunteers, 88
OSCE, 495, 1104, 1117, 1143, 1147, 1153, 1154, 1163, 1180, 1184, 1199, 1217, 1225, 1246, 1247, 1253, 1257, 1259
Outbidding, 572, 777
Pakistan Tehreek-i-Insaf, 277
Palestine Liberation Organization (PLO), 84, 88, 208, 241, 517, 629, 630, 768, 772, 773, 774, 775, 777, 779
Palestinian Authority (PA), 768, 773
Palestinian Islamic Jihad (PIJ), 517, 768
Palestinians, 126, 149, 240, 241, 242, 255, 664, 768, 772, 773, 774, 775, 776, 777, 779, 780, 792, 823
Papazoglou, Konstantinos, 955, 959
Paris, 9, 93, 249, 252, 296, 298, 302, 303, 360, 416, 418, 451, 486, 490, 794, 796, 802, 805, 850, 1030, 1032, 1040, 1046, 1047, 1048, 1051, 1052, 1053, 1054, 1055, 1056, 1145, 1183, 1185, 1203, 1204, 1211
Passenger screening, 706, 790, 793, 795, 796, 798, 806, 807, 854
Passive Prevention, 30
Past Attacks on Educational Institutions, 167
Patrols, 1040
Peacebuilding, 1125, 1156, 1210, 1213, 1241
Peeters, Rik, 14, 1153, 1184
Perceptions, 214, 973, 974, 978, 982, 1171, 1172, 1182, 1185, 1190, 1191, 1205, 1207, 1249
Perpetrators of Violence, 20, 143, 150, 151, 155, 156, 568, 685
Perry, Ronald W., 977, 983
Personal grievance, 151, 373, 378, 792
Petraeus, David, 81, 123, 124
Pfefferbaum, Betty, J., 954, 959
PFLP, 629, 775, 777, 791, 792, 794
Phalangists, 772
Pinker, Steven, 19
Plan of Action, 9, 166, 295, 1103, 1104, 1105, 1106, 1107, 1108, 1109, 1110, 1111, 1112, 1113, 1114, 1115, 1116, 1117, 1118, 1119, 1120, 1121, 1123, 1124, 1125, 1126, 1132, 1136, 1141, 1144, 1145, 1146, 1148, 1150, 1151, 1156, 1158, 1218, 1219, 1258
Police, 21, 22, 171, 249, 300, 404, 431, 542, 601, 625, 631, 664, 666, 668, 671, 687, 707, 750, 805, 807, 821, 822, 858, 860, 941, 955, 959, 976, 990, 999, 1003, 1011, 1016, 1017, 1019, 1025, 1044, 1051, 1055, 1140, 1162, 1166, 1172, 1180, 1188, 1196, 1197, 1199, 1203, 1217, 1225, 1226, 1227, 1228, 1233, 1242, 1248, 1249, 1254
Recruitment, 5, 244, 246, 396, 398, 399, 400, 401, 403, 404, 408, 412, 413, 415, 419, 421, 423, 424, 426, 542, 597, 600, 609, 1037, 1154, 1157, 1165, 1173, 1182, 1185, 1188, 1190, 1191, 1194, 1195, 1197, 1198, 1200, 1203, 1211, 1245, 1247, 1254, 1256

Red Brigades, 78, 111, 150, 208, 629, 802

Reddit, 368, 1034, 1050

Refugee Camps, 4, 238, 1195, 1198

Refugees, 183, 240, 241, 242, 243, 244, 246, 249, 250, 256, 308, 487, 955, 959, 977, 1012, 1023

Regional Refugee and Resilience Plan (3RP), 246, 247

Rehabilitation, 181, 210, 224, 230, 231, 375, 1172, 1186, 1246

Reinares, Fernando, 802, 1051, 1056, 1234

Religion, 272, 379, 1050, 1055, 1057, 1174, 1183, 1205, 1214

Repatriation, 247

Repression, 1014, 1022, 1154, 1161, 1173, 1244, 1252


Respect, 215, 221, 1150, 1225

Revenge, 9, 212, 1027, 1028, 1029, 1030, 1036, 1038, 1039, 1040, 1041, 1042, 1043, 1044, 1045, 1047, 1051, 1053, 1054, 1056, 1058

Richard Reid, 654, 796, 850

Richardson, Louise, 671, 1015, 1016, 1018, 1020, 1023, 1024, 1025, 1026, 1193

Right-wing extremism, 24, 152, 153, 297, 299, 302, 303, 307, 308, 342, 343, 682, 687, 696, 1045, 1081, 1203, 1207

Risk Assessment, 978, 983, 1012, 1023, 1186, 1190, 1223, 1224, 1235, 1246

Rocket-Propelled Grenades (RPGS), 510

Rohingya, 246, 370

Romaniuk, Peter, 16, 1155, 1179, 1209, 1216, 1218, 1240, 1247, 1252

Ross, Gina, 957, 959

Rule of Law, 28, 1107, 1112, 1191, 1246

Rumiyah, 362, 827, 848

Russian Federation, 741, 746, 1147

Rwanda, 140, 145, 146, 147, 148, 149, 242

Sabotage, 115, 116, 117, 118, 509, 516, 519, 541, 545, 654, 766, 790, 792, 793, 794, 796, 799, 800, 803, 804, 805, 806, 808, 846, 850, 855, 860

Salafism, 290, 305, 312, 320, 407, 413

Sampson, Nicos

SARS, 985, 994, 996, 1005, 1006, 1007, 1017

Saul, Jack, 957, 960

Schlenger, William E., 953, 960

Schorr, John K., 956, 960

Schuster, Mark A., 953, 960

Scotland, 626, 632, 851

Screening, 637, 807, 1175, 1228, 1234, 1235

Securitization, 1012, 1020, 1194, 1229, 1235

September 11, 2001 (9/11 attacks), 2, 51, 56, 63, 151, 154, 279, 396, 431, 450, 532, 568, 569, 576, 629, 631, 665, 765, 770, 771, 779, 790, 794, 796, 798, 809, 824, 847, 873, 894, 933, 934, 935, 936, 937, 945, 948, 950, 967, 1032, 1045

Shame, 154, 211, 936, 948, 966

Siegrist, Michael, 980, 983

Signal, 368

Sina Weibo, 368

Sinn Féin, 1038, 1048, 1051, 1056
Situational Crime Prevention (SCP), 3, 49, 50, 51, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 705, 706, 707, 708, 711, 1162, 1165, 1166, 1168, 1169, 1172, 1174, 1175, 1252

Skype, 365
Slone, Michelle, 955, 960
Slovic, Paul, 978, 983, 1225
Snopes.com, 377
Social Justice, 28, 1107, 1171, 1173, 1175, 1229, 1231, 1234, 1237, 1250, 1253
Social Media, 5, 183, 217, 358, 359, 367, 410, 419, 601, 979, 1110, 1191, 1192, 1193, 1194, 1200, 1206, 1232, 1248, 1252, 1257
Soft targets, 533, 817, 818
Soldiers of Odin, 1035, 1050, 1053, 1055
Solomon, Zahava, 954, 960
Somalia, 117, 150, 168, 173, 245, 247, 513, 514, 516, 640, 797, 845, 846, 847, 851, 852, 1206
Somasundaram, Daya, 954, 960
Somer, Eli, 954, 960
SoundCloud, 364
South African, 82, 212, 860
South Sudan, 373, 455
Southeast Asia, 5, 171, 172, 182, 184, 358, 361, 373, 379, 992, 993, 995, 1001, 1002, 1007, 1012, 1013, 1020, 1022, 1024, 1213, 1244
Sovereignty, 1050, 1053
Spain, 112, 167, 170, 224, 249, 250, 251, 252, 257, 453, 478, 629, 801, 802, 805, 848, 1143, 1234, 1259
Sports, 177, 179, 901, 1143, 1152, 1214, 1216, 1220
Sri Lanka, 113, 170, 283, 368, 369, 447, 452, 511, 538, 768, 769, 797, 803, 933, 938, 950, 954, 960, 993, 1041, 1052, 1053, 1177, 1257
Stress, 935, 945, 953, 954, 955, 956, 958, 959, 960, 961, 962, 980, 981, 1237
Students, 4, 175, 178, 179, 183, 184, 185, 270, 417, 944, 1171

Sudan, 86, 117, 147, 243, 373, 455, 512, 515, 796
Suicide attack, 7, 36, 119, 410, 428, 492, 516, 627, 629, 709, 711, 764, 765, 766, 767, 768, 769, 770, 771, 774, 775, 776, 777, 778, 779, 780, 795, 803, 804, 824
Suicide bombing, 151, 153, 155, 492, 595, 707, 764, 765, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 790, 805, 937, 950, 1041, 1152, 1168, 1171, 1189
Surface-to-air missiles, 121, 797
Surface-To-Air Missiles (SAM), 852
Surveillance, 30, 220, 632, 825, 1163, 1173, 1174, 1255
Sustainable Development Goals, 1127, 1133, 1134, 1203
Target Hardening, 708, 1224
TATP [Triacetone Triperoxide – explosive], 686, 687, 851
Tech Against Terrorism, 367
Tehreek-i-Taliban Pakistan, 279
Telegram, 358, 365, 366, 368, 369, 421, 602, 873, 1036
Terrorism Prevention, xxv, xxix, 1, 2, 3, 8, 9, 13, 15, 23, 26, 27, 28, 29, 30, 31, 54, 55, 56, 77, 379, 454, 578, 746, 816, 817, 830, 952, 960, 1103, 1123,
Wolmer, Leo, 956, 961
Women, 182, 308, 314, 320, 459, 1126, 1143, 1145, 1152, 1153, 1165, 1189, 1195, 1196, 1199, 1206, 1212, 1213, 1215, 1219
World Bank, 146, 445, 454, 538, 994, 995, 996, 1000, 1001, 1008, 1015, 1020, 1023, 1161, 1164
World Trade Center, 568, 631, 633, 710, 795, 809, 956, 959, 967, 978, 986, 1011, 1020, 1025
Yazidis, 173, 247
Yemen, 2, 224, 230, 245, 452, 512, 514, 516, 538, 631, 640, 666, 747, 853, 1019, 1124, 1131
Youth, 169, 172, 175, 179, 183, 244, 251, 254, 308, 312, 890, 901, 1037, 1108, 1126, 1137, 1143, 1145, 1168, 1175, 1176, 1179, 1183, 1184, 1185, 1186, 1193, 1194, 1195, 1196, 1198, 1200, 1206, 1209, 1212, 1213, 1217, 1218, 1239
YouTube, 152, 177, 183, 303, 358, 362, 368, 369, 373, 421, 595, 596, 599, 606, 608, 685, 874, 1186, 1210
Za'tari Camp, 246
Zaire, 240, 242
ZAKA, Identification of disaster victims, 933, 937, 939, 950, 954, 960
Zarqawi, Abu Musab al-, 117, 418, 535, 565, 848
Zawahiri, Ayman, 155, 496, 565
Zedong, Mao, 115, 116, 123, 517
HANDBOOK OF TERRORISM PREVENTION AND PREPAREDNESS

With nearly 40 contributors and 35 chapters, this Handbook offers more than a thousand pages of comprehensive overview of current thinking on alternative approaches to countering terrorism, based on anticipation and the reduction of risk factors. Informed by insights from criminology, counter-insurgency and conflict studies as well as analysis of politicides, factors contributing to radicalization, violent extremism and terrorism are explored.

Three levels of prevention are introduced:

- Upstream prevention: reducing the risk of the formation of a terrorist group or organization;
- Midstream prevention: reducing the risk of such a group or organization being able to prepare a terrorist campaign; and
- Downstream prevention: reducing the risk of execution of individual terrorist operations by foiling and deterring these.

Preparedness is conceptualized as taking proactive and pre-emptive measures to reduce risks and threats and, if that turns out to be insufficient, reduce the negative impact of terrorist attacks through a set of planned precautionary measures aimed at strengthening governmental readiness and societal resilience.

Alex P. Schmid is a Research Fellow of the ICCT and a former professor of Leiden University, Erasmus University and the University of St. Andrews. While working for the United Nations, he was Officer-in-Charge of the Terrorism Prevention Branch in Vienna. He is Editor-in-Chief of ‘Perspectives on Terrorism’ and Director of the Terrorism Research Initiative, a consortium of institutes and scholars dedicated to enhance security through collaborative research.

ICCT
International Centre for Counter-Terrorism - The Hague

www.icct.nl