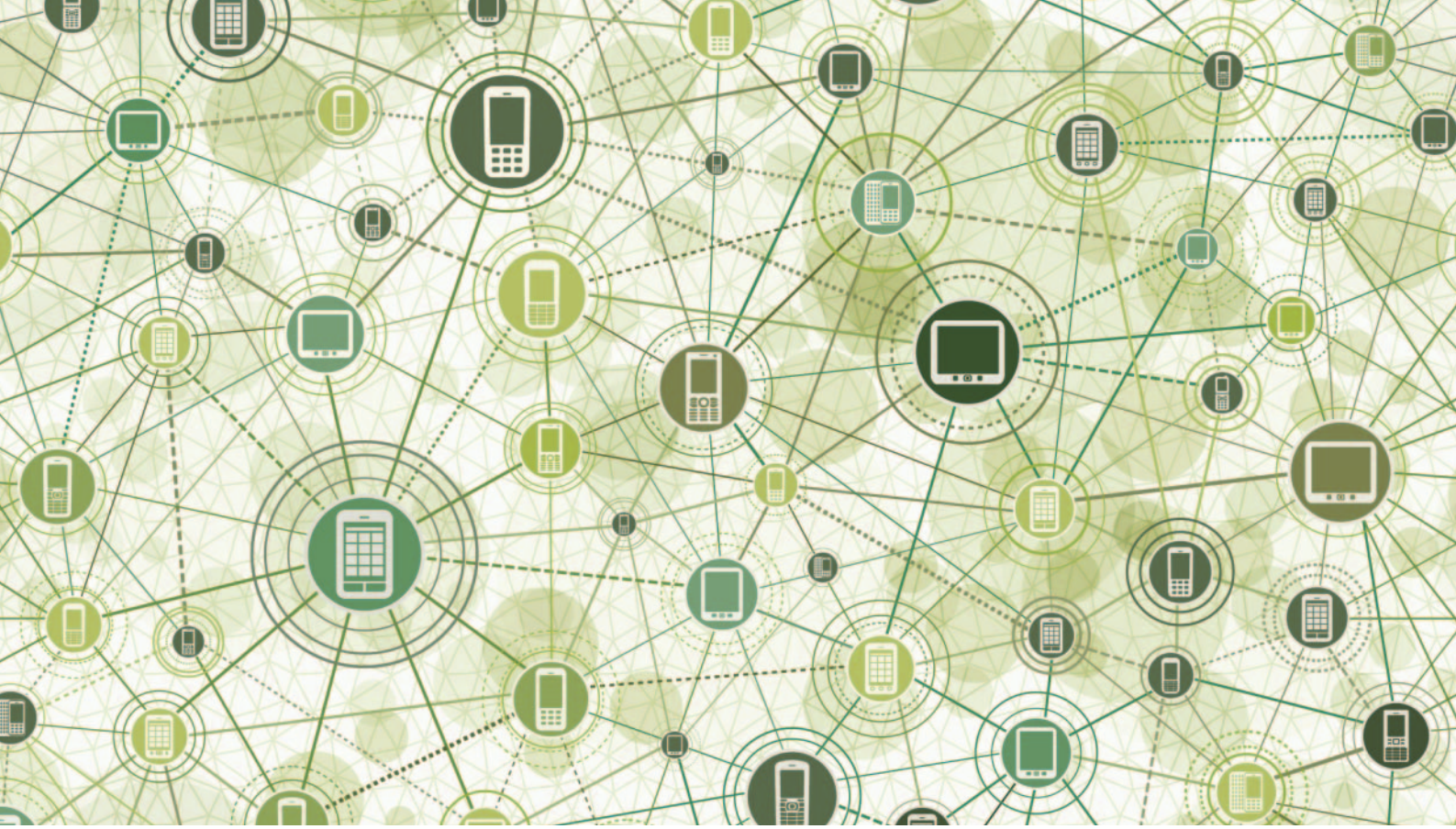
This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.



Radicalisation in the digital era

The use of the internet in 15 cases of terrorism and extremism

Ines von Behr, Anaïs Reding, Charlie Edwards, Luke Gribbon

RAND EUROPE

RAND EUROPE

Radicalisation in the digital era

The use of the internet in 15 cases of terrorism and extremism

Ines Von Behr, Anaïs Reding, Charlie Edwards, Luke Gribbon

RAND Europe is an independent, not-for-profit policy research organisation that aims to improve policy and decisionmaking for the public interest though research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND OFFICES

SANTA MONICA, CA • WASHINGTON, DC

PITTSBURGH, PA • NEW ORLEANS, LA • JACKSON, MS • BOSTON, MA

DOHA, QA • CAMBRIDGE, UK • BRUSSELS, BE

www.rand.org • www.rand.org/randeurope

Preface

We live in a digital era. In the UK alone 85 per cent of homes have internet access. As society increasingly embraces the internet, so opportunities for those wishing to use it for terrorism have grown. The internet offers terrorists and extremists the capability to communicate, collaborate and convince. In recent years, European policymakers, practitioners and the academic community have begun to examine how the internet influences the process of radicalisation: how a person comes to support terrorism and forms of extremism associated with terrorism.

Many of the policy documents and academic literature in this area focus on online content and messaging, rather than exploring how the internet is used by individuals in the process of their radicalisation. The reason for this focus is relatively straightforward. Gaining access to terrorists (those convicted under UK terrorism legislation) or extremists (identified by the police and multi-agency partners based on an assessment of risk) is extremely difficult. Obtaining primary data relating to these individuals' cases held in court records or by the police is labour-intensive and a logistical challenge. However, empirical research is needed in order to rigorously test assertions about radicalisation and formulate evidence based approaches to addressing challenges associated with radicalisation.

In order to begin to address this gap and develop the evidence base in the field, this study is based on primary data drawn from a variety of sources: evidence presented at trial, computer registries of convicted terrorists, interviews with convicted terrorists and extremists, as well as police senior investigative officers responsible for terrorist investigations. The sample size is small: a symptom of both the limited number of individuals willing to speak with researchers in this field, and the challenge of collecting data on such a sensitive topic where information in the public domain is limited.

RAND Europe is an independent not-for-profit policy research organisation that aims to improve policy and decision-making in the public interest, through research and analysis. RAND Europe's clients include European governments, institutions, non-governmental organisations and firms with a need for rigorous, independent, multidisciplinary analysis.

For more information about this project or RAND Europe please contact:

Ines von Behr (ivonbehr@rand.org)

RAND Europe
Rue de la Loi 82
Brussels 1040
Belgium
Tel. +32 2669 2400

RAND Europe
Westbrook Centre, Milton Road
Cambridge CB4 1YG
United Kingdom
Tel. +44 1223 353 329

Table of Contents

Figures

Tables

Acknowledgements

We are enormously grateful to the Association of Chief Police Officers (ACPO), the Office for Security and Counter Terrorism (OSCT) and Home Office for their support, guidance and help with this study. In particular we would like to thank Assistant Chief Constable John Wright, National Coordinator of Prevent and Siobhan Peters, Director of Prevent, OSCT.

We owe a particular debt of gratitude to the police Senior Investigative Officers (SIOs) across the UK who agreed to spend hours with us going through individual cases. Their determination to learn from past investigations as well as explore future challenges in policing terrorism online ensured the research team met the right people and had access to the most relevant material.

At RAND Europe our thanks go to Éanna Kelly, Ben Baruch, Kate Robertson, Jennifer Rubin, Richard Warnes and Rebecca Schindler for their support, editing and clarity of thinking.

Abbreviations

ACPO	Association of Chief Police Officers
AQ	Al Qa'ida
CONTEST	The United Kingdom's Strategy for Countering Terrorism
CPS	Crown Prosecution Service
CSP	Communication Service Provider
CTIRU	Counter Terrorism Internet Referral Unit
CTU	Counter Terrorism Unit
EC	European Commission
ENER	European Network of Experts on Radicalisation
EU	European Union
ICT	Information and communication technology
ISP	Internet Service Provider
JHA	Justice & Home Affairs Council, Council of the EU
OSCT	Office for Security and Counter Terrorism
RAN	Radicalisation Awareness Network
SIA	Security and Intelligence Services
SIO	Senior Investigative Officer
TACT	UK Terrorist legislation
WiMax	Worldwide Interoperability for Microwave Access
WWW	Worldwide web

Executive Summary

The internet has brought extensive change in peoples' lives. It has revolutionised how we communicate and simplified the way we create networks among like-minded individuals. We live in an era in which 84 per cent of the EU population use the internet daily, including 81 per cent of whom access it from home (Eurostat, 2012).

This development has led to important changes in the organisation and functioning of society, and as violent extremists and terrorists form part of this society, it is widely assumed that the internet plays a particular role as a tool of radicalisation (Aly, 2010; Awan, 2007; Friedland, 2009; O'Rourke, 2007; Tucker, 2010). There is, however, very limited evidence available to assess this assumption.

Testing hypotheses from the literature against primary data: the case of 15 terrorists and extremists

This paper presents the results from exploratory primary research into the role of the internet in the radicalisation of 15 terrorists and extremists in the UK. The 15 cases were identified by the research team together with the UK Association of Chief Police Officers (ACPO) and UK Counter Terrorism Units (CTU). The research team gathered primary data relating to five extremist cases (the individuals were part of the Channel programme, a UK government intervention aimed at individuals identified by the police as vulnerable to violent extremism), and ten terrorist cases (convicted in the UK), all of which were anonymised. The team conducted interviews with the Senior Investigative Officers (SIOs) involved with the terrorists and Channel participants, and investigated the individuals' online behavior from data recovered by the police directly from the individuals' computers. The team then conducted a literature review and developed a number of hypotheses or assertions found in the literature on the role of the internet in the process of radicalisation. These hypotheses were tested using primary data from the above mentioned 15 cases.

The following five hypotheses identified in the literature were:

1. The internet creates more opportunities to become radicalised.
2. The internet acts as an 'echo chamber': a place where individuals find their ideas supported and echoed by other like-minded individuals
3. The internet accelerates the process of radicalisation.
4. The internet allows radicalisation to occur without physical contact.
5. The internet increases opportunities for self-radicalisation.

Findings

Evidence from the primary research conducted confirmed that the internet played a role in the radicalisation process of the violent extremists and terrorists whose cases we studied. The evidence enabled the research team to explore the extent to which the five main hypotheses that emerged from the literature in relation to the alleged role of the internet in radicalisation held in these case examinations. The summary findings are briefly presented here and discussed in greater detail in the full report that follows:

The internet creates more opportunities to become radicalised

Firstly, our research supports the suggestion that the internet may enhance opportunities to become radicalised, as a result of being available to many people, and enabling connection with like-minded individuals from across the world 24/7. For all 15 individuals that we researched, the internet had been a key source of information, communication and of propaganda for their extremist beliefs.

The internet acts as an 'echo chamber'

Secondly, our research supports the suggestion that the internet may act as an 'echo chamber' for extremist beliefs; in other words, the internet may provide a greater opportunity than offline interactions to confirm existing beliefs.

The internet accelerates the process of radicalisation

This evidence does not necessarily support the suggestion that the internet accelerates radicalisation. Instead, the internet appears to facilitate this process, which, in turn, may or may not accelerate it.

The internet allows radicalisation to occur without physical contact

The evidence does not support the claim that the internet is replacing the need for individuals to meet in person during their radicalisation process. Instead, the evidence suggests that the internet is not a substitute for in-person meetings but, rather, complements in-person communication.

The internet increases opportunities for self-radicalisation

The evidence from this research does not support the suggestion that the internet has contributed to the development of self-radicalisation. In all the cases that we reviewed during our research, subjects had contact with other individuals, whether virtually or physically.

Recommendations and areas of future research

The results from this study are based on a small number of cases and because they constitute a convenience sample, their narratives will not necessarily reflect the way in which *all* violent extremists and terrorists use the internet during their radicalisation; however, it nonetheless allows us valuable insights relatively unexplored until now, and highlights the importance of cross-referencing, validating and challenging hypotheses from the literature with empirical evidence.

The first hand evidence gathered for this report confirmed that the internet was widely evident in the radicalisation process of violent extremists and terrorists who formed the sample for this study. The evidence enabled the research team to delve into this further, and to explore whether the five main hypotheses that emerged from the literature in relation to the supposed role of the internet in radicalisation held true in the cases studied. As indicated above, the primary evidence obtained in this

research supports the suggestion that *the internet may enhance opportunities to become radicalised*. While our research supports the suggestion that the internet has expanded opportunities for radicalisation and that it provides a means through which to filter material that is consistent with one's beliefs (the internet as an 'echo chamber'), our findings challenged other suggestions emerging from the literature. The detailed information to which the research team gained access suggested a sometimes different picture to some of the hypotheses put forward in the literature. The study therefore demonstrates the importance of gathering first hand evidence, or conducting primary research, to be able to gain a more complete picture of the role of the internet in radicalisation. The internet is one aspect of radicalisation, and it is essential for future research to look both online and offline to be able to understand the process as a whole.

Our findings suggest that this and other primary research could usefully inform the development of new strategies and policies, as well as the allocation of resources to address new security challenges raised by the internet and its role in radicalisation. This enhancing of understanding and informing policy and practice could be achieved through public-private collaborations, training and/or other initiatives.

1. Introduction

This chapter sets out the purpose of the study and explains the structure of the report. It begins by defining key terms before highlighting the importance of the internet as a domain of activity for both radicalisation and terrorism. In this section we provide a short overview on how the policy world has responded to online radicalisation, and problems policymakers face in dealing with this phenomenon.

Chapter 1 highlights gaps in public domain evidence on individuals' engagement with the internet in the course of their radicalisation. It then outlines the importance of acquiring the necessary empirical evidence on individuals' use of the internet in the course of radicalisation, in order to both balance the existing literature and to provide policymakers with useful insights to inform future policy, strategy and actions in this field.

1.1. Report structure

Subsequent chapters are structured as follows:

- Chapter 2 outlines the methodological approach of this study, discussing the research questions, methods and approaches to the research. We pay particular attention to the collection of primary data on individuals' use of the internet and the inherent challenges and obstacles faced. A triangulation approach to primary data collection was followed combining: semi-structured interviews with the subjects of our case studies; semi-structured interviews with police senior investigative officers or other staff closely involved with the individual's case; and a review of the available information on the case, including trial transcripts (in instances where documents had been made available to the team) and relevant computer registries.
- Chapter 3 focuses on the analysis of the academic literature, and discusses the state of the current academic field. We draw five main hypotheses from the literature which play an essential role in the debate around the phenomenon of online radicalisation.
- Chapter 4 examines 15 individual cases for which primary data has been collected. The cases are based in the UK and include both males and females, divided into two categories: category A contains a mix of offenders convicted under UK terrorism legislation and former members of proscribed terrorist groups who have disengaged from terrorism. Category B contains cases of individuals who have been identified by the police and multi-agency partners as vulnerable to extremism and are, or have been part of, an intervention programme. Following brief descriptions of these individuals' case histories, the chapter provides a comparative analysis and insights

clustered around five hypotheses (as identified in chapter 3) relevant to the key issues and experiences of the internet's role in their radicalisation.

- Chapter 5 presents a brief outline of relevant implications and recommendations for further research on online radicalisation. It also includes some potential recommendations for the policy community and reflections on how to use the web to counter radicalisation building on the results of this study.

1.2. Defining what we mean by the internet, terrorism, extremism and radicalisation

The internet plays a central role in many people's everyday lives and while some argue that it is associated with growing isolation, others suggest that it is associated with greater sociability. As Castells and Cardoso (2005) argue, "The network society is a hyper social society, not a society of isolation (p. 11)."

Our research suggests that important terms in consideration of this issue, 'the internet', 'radicalisation' or 'online radicalisation,' are left at times under-defined in both policy and academic literature. This ambiguity of terms is worth highlighting from the outset as defining what constitutes the internet and radicalisation has an important bearing both on research and on the scope of policy responses.

In one of the few comments on this issue of definitions, Cornish (2008, 3) notes

"the challenge of identifying the digital footprint of Internet-based radicalisation invites discussion as to the very nature of the Internet. (page 3)"

For the purpose of this study we will define the *internet* as including all communication, activity or content which takes place or is held on the world wide web (www) and cloud structures. This includes new online developments such as social media and networks.

In this report we draw on the UK Terrorism Act 2000 definition of *terrorism*[1] as an action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system (Part 1(1)). According to this definition, the use or threat must be designed to influence the government or to intimidate the public, and is made for the purpose of advancing a political, religious or ideological cause.

Extremism is defined by the British Government as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs (*Prevent* Strategy, 2011, p.107). The definition of *radicalisation* is contested because of the many positive or non-harmful connotations that 'radical' and 'radicalism' have. Whilst we acknowledge this debate, this study has a different focus and therefore adopts the UK Government definition applied in the *Prevent* strategy: "radicalisation is the process by which a person comes to support terrorism and forms of extremism leading to terrorism" (Prevent strategy, Home Office 2011). We adopt a definition of 'online radicalisation' that is aligned: "a process whereby individuals through

[1] UK Terrorism Act 2000: http://www.legislation.gov.uk/ukpga/2000/11

their online interactions and exposures to various types of internet context, come to view violence as a legitimate method of solving social and political conflicts" (Bermingham 2009).

1.3. The internet as a domain of activity for terrorist activities

The so called information revolution, with the unexpected rise of the internet since the 1990s, has clearly been of growing societal significance. The internet offers terrorists and extremists the same opportunity and capability that it does for the rest of society: to communicate, collaborate and convince. There are already significant quantities of radical materials available online, and this volume is growing daily. The following table 1 illustrates today's wide-spread availability of material pertinent to extremism and terrorism on-line:

Table 1: Google search for examples of critical keywords

Search Term	Number of Results
"how to make a bomb"	1,830,000
"Salafi publications"	46,200
"beheading video"	257,000

Source: RAND Europe's own observations (based on web results for selected search terms)

An analysis of UK policy documents and interviews with SIOs (senior investigating officers) confirms that the internet plays a part in almost every national security investigation conducted by the security and intelligence agencies and police in the UK. Terrorism cases in the UK without a 'digital footprint' are increasingly rare.

Whilst terrorists and extremists can indeed use the internet for a myriad of purposes (disseminating propaganda and information to radicalise individuals, operational planning and fundraising) – to what extent does activity online influence offline behaviour and vice versa? We examine this question in order to understand the importance (or lack thereof) of the internet for radicalisation. What role does the internet play with regard to the apparent phenomenon of online radicalisation? Is the internet merely a source of inspiration? Does it accelerate the radicalisation process? Does it translate into action? These questions are explored in subsequent chapters through the 15 cases that form the primary research for this study.

1.4. Policy responses to online radicalisation

The malignant potential of the internet has become a primary concern for policymakers and changed the way in which national security threats are investigated. Governments are increasingly aware of the importance of the internet in radicalisation. Before describing our research and the findings from our cases, it is helpful to consider how the policy community is responding to the role of the internet in radicalisation. This will set the context for further thinking on policy approaches discussed in the last chapter.

1.4.1. UK Government's response to internet radicalisation

The British government has been at the forefront of tackling terrorist use of the internet. Since July 2006, when the British government made public its strategy to counter international terrorism (CONTEST, 2006), the internet has been identified as a domain "where many types of radical views are strongly promoted" (UK Home Office, 2006). The growth of the use of the internet, with its ability to connect people and to facilitate dissemination of information and ideas, has had a significant impact on the accessibility and flow of radical ideas.

In March 2009 the government published a revised version of CONTEST which set out a more sophisticated approach to online counter-terrorism. However, the document acknowledged that "the internet presents significant challenges for CONTEST in general" (UK Home Office, 2009).

The new approach places a premium on working with filtering companies, disrupting the use of the internet for extremist messaging and increasing the use of the internet to promote alternative views to the radicalised messages that may otherwise be accessed (Home Office 2009). The strategy also argued for the development of specialist units to counter the threat of terrorism from online sources and material.

In 2010 the Counter Terrorism Internet Referral Unit (CTIRU)[2] was launched within the Association of Chief Police Officers (ACPO)[3]. This unit removes or modifies unlawful internet content, identifies the individuals responsible for posting such material, and supports the police counter-terrorism network in investigating and prosecuting terrorist or radicalising activity online. It proactively scans the web for content that promotes or glorifies terrorism,[4] as well as acting on referrals from citizens and public bodies. Flagged sites' content is reviewed by specialists and where material is deemed to breach UK law, CTIRU seeks to remove the site from the internet in collaboration with internet service providers (ISPs).

CTIRU develops and shares new technologies to assess and process internet content, and to improve the effectiveness of the police response to unlawful material. From February 2010 to September 2012 there were approximately 3,100 referrals to CTIRU resulting in 410 take-downs of material (a 13.2 per cent strike rate). Between July and September 2012 there were 341 referrals in total, with 232 (68 per cent) from the general public via Directgov[5] (see Figure 1 and Figure 2). The most frequently-referred sites were Facebook, Twitter and Blogger and/or Blogspot. There were 105 removals (31 per cent) during this same period.

---

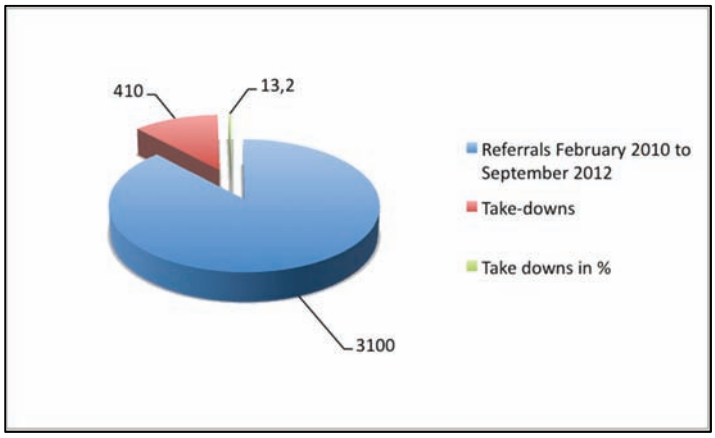
[2] The Counter Terrorism Internet Referral Unit: http://www.acpo.police.uk/ACPOBusinessAreas/PREVENT/TheCounterTerrorismInternetReferralUnit.aspx

[3] The Association of Chief Police Officers (ACPO): http://www.acpo.police.uk/Home.aspx

[4] As defined by the relevant provisions of section 58 of the Terrorism Act 2001, and sections 1–3 of the Terrorism Act 2006.

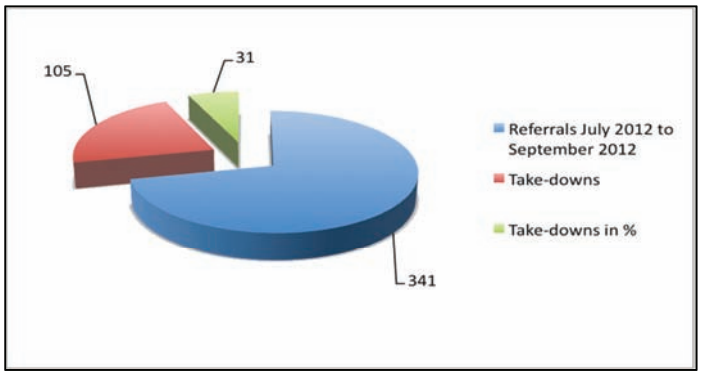
[5] Directgov was the British government's digital service and provided a single point of access to public sector information and services. The site was replaced by the new Gov.uk website on 17 October 2012.

Figure 1: Referrals (total numbers)/take-downs (total numbers and percentage) February 2010 - September 2012



Source: RAND Europe interview with CTIRU, September 2012

Figure 2: Referrals (total numbers)/take-downs (total numbers and percentage) July 2012 - September 2012



Source: RAND Europe interview with CTIRU, September 2012

For reasons of security and safety, accessibility and anonymity, terrorists and extremists have shifted many of their activities from public spaces (such as mosques in the case of Islamist extremist groups) to private residences, and now to personal computers and tablets. According to Charles Farr, Director General of the Office for Security and Counter Terrorism (OSCT):

'violent radicalisation in mosques or other religious institutions comprises no more than 1% or 2% of the total cases of radicalisation (House of Commons Home Affairs Committee, 2012)'.

Therefore, the process of radicalisation is becoming increasingly covert, posing problems for the security and intelligence agencies and local police forces in the UK. This shift in terrorist behaviour largely reflects society's expanding digital footprint, where everyday activities move seamlessly between online and offline domains. The shift in activity to the internet supports the observation of the former Chief Constable of West Yorkshire and ACPO lead on *Prevent*, Sir Norman Bettison, that "the internet features in most, but not all, terrorism cases" (House of Commons Home Affairs Committee, 2012).

In response to this shift, engaging with technology industries has been a priority for the British government. Communication service providers and ISPs set their own terms of use, and some have introduced ways of identifying content which might breach legal guidelines. For example, YouTube has introduced a 'promoting terrorism' referral flag for videos deemed to be of a terrorist nature[6], while AOL has increased the visibility of the Metropolitan Police Anti-terrorism Hotline[7] by ensuring that it is presented when certain specific search requests are entered (UK Home Office, 2011).

Following a review of the *Prevent* strategy, in 2011 a new version of the strategy was published. The revised strategy included a section on the internet in its own right, while the internet was a cross-cutting theme throughout the document. The strategy stated:

> '[T]he internet has transformed the extent to which terrorist organisations and their sympathisers can radicalise people in this country and overseas. It enables a wider range of organisations and individuals to reach a much larger audience with a broader and more dynamic series of messages and narratives. It encourages interaction and facilitates recruitment. The way people use the internet also appears to be conducive to these processes (UK Home Office, 2011).

The revised strategy stated that more work was needed, including:

- The roll-out of a filtering product across government departments, agencies and statutory organisations;
- Determining the extent to which effective filtering is in place in schools and public libraries;
- Directing further resources to a police agency, the CTIRU, to take down web sites which breach legal guidelines relating to extremist material inciting hatred or furthering radicalisation;
- Increasing the number of referrals to the CTIRU and developing CTIRU's technical, investigative and international capabilities;
- Increasing the UK's international work, both with the US, the EU and EU Member States to explore self-regulatory measures to tackle terrorist use of the internet and seek to optimise existing projects and initiatives; and
- Prioritising projects to disrupt terrorist and radicalising material on the internet and radicalisers working in this country (UK Home Office, 2011).

1.5. Terrorism, the role of the internet and policy responses in Europe beyond the UK

In addition to the UK context discussed above, wider Europe's terrorist threat is also associated with scrutiny of the role of the internet. Examples of the influence of the internet in terrorist incidents include a June 2012 Belgian case, where a court rendered a decision concerning five persons charged with terrorism-related offences. The subjects were charged with managing websites that were used for

[6] Huffington Post, 2010.

[7] Anti-Terrorist Hotline: http://content.met.police.uk/Article/AntiTerrorist-Hotline/1400006265916/1400006265916 [Last accessed 23/08/2013].

recruiting people for armed struggle. A link to al-Qa'ida appeared from the content of these websites (Europol Trend Report 2013:14). An arrest was made by the Dutch police in Amsterdam in March 2012, in which a suspect had also been searching the Internet for manuals on how to make explosives (2013:17). Another example occurred in April 2012, when an Italian convert to Islam was arrested, having been actively engaged in spreading via the internet terrorist propaganda and documents on training in the use of weapons and explosives (2013:19).

1.5.1. The EU approach with regard to online radicalisation

The EU's position on internet radicalisation can largely be summarised as a strategy of preventing access to terrorists in an attempt to disrupt recruitment efforts. The EU's overall policy on terrorism is formalised through its 2002 Framework Decision on combating terrorism - a policy instrument that seeks to define the EU position on terrorism and provide scope to the EU and Member States to combat terrorism both within the EU and abroad (Council of the European Union, 2002).

From 2005 onwards, the European Commission (EC) and the Justice and Home Affairs (JHA) Council began placing a high priority on curbing online radicalisation (Ryan, 2007). Disrupting the activities of networks by examining 'ways to impede terrorist recruitment using the internet' became a key EU policy objective (Council of the EU, 2005a). Further strategies announced the intention to explore possibilities to address factors conducive to violent radicalisation (European Commission, 2006):

- The European Council supported an information portal called the 'Check the Web' initiative, which aimed at strengthening cooperation and sharing the task of monitoring and evaluating open internet sources on a voluntary basis[8].
- A clause was included in the Audiovisual Media Services (AMS) Directive (2010) which stated that Member States shall ensure by appropriate means that 'audiovisual media services provided by media service providers under their jurisdiction do not contain any incitement to hatred based on race, sex, religion or nationality'.
- In 2010, the EU-funded 'Clean IT project'[9] was established to start a constructive dialogue between governments, businesses and civil society to explore how to reduce the terrorist use of the internet. This dialogue resulted in a set of general principles and an overview of possible best practices aimed at reducing terrorist use of the internet.
- The Radicalisation Awareness Network (RAN) is a network within the Home Affairs office of the EU which seeks to aid and facilitate information sharing amongst 'first-liners' – people directly engaged with at-risk individuals or groups – within the EU.[10] First-liners include social workers, teachers, police, academics, and NGO's. RAN has particularly focused on the internet, with a May 2013 meeting addressing the role of the internet in radicalisation (RAN, 2013).

---

[8] 'Check the Web' initiative: http://register.consilium.europa.eu/pdf/en/07/st08/st08457-re03.en07.pdf [Last accessed 02/09/2013].

[9] The Clean IT project: http://www.cleanitproject.eu [Last accessed 02/09/2013].

http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/index_en.htm [Last accessed 23/08/2013].

- Workshops on using the internet to foster tolerance and moderation, such as the December 2012 High Level Conference hosted by the RAN (RAN, 2012) seek to exchange knowledge and best-practice between EU-level organisations and the private sector. The conference proposed examples of good practice in implementing 'counter-narratives' on the internet which challenge extremist discourse online, and explored ways in which the EU can collaborate with the private sector to combat radicalisation online.
- The EU Internal Security Strategy in Action's 'second step' lists several actions that are taken to address radicalisation. Amongst these was the creation of RAN, but also a ministerial conference on the prevention of radicalisation, and a 'handbook of actions and experiences' to support the efforts of Member States.
- The European Network of Experts on Radicalisation (ENER) is an EU-instituted organisation, hosted through the UK-based Change Institute, which establishes a network of organisations and experts on the issues of radicalisation. The network is an attempt to deepen the Commission's understanding of radicalisation through publications, seminars, and workshops.
- Finally, the EU notes that the bulk of counter-radicalisation work takes place at a local-community level, and is thus best handled at a national level. The EU nevertheless offers a framework to coordinate national policies and facilitate information sharing on best-practices.

1.6. The academic focus: limited evidence on online radicalisation

In terms of the evidence base, a review of literature undertaken for this study suggests that views are divided and the empirical evidence base is limited. Whilst many studies have emphasised the internet's significance (Stenerson 2008, Bakker 2007, Gray 2010, Zeng et al. 2011), others have concluded that the internet 'does not appear to play a significant role in al-Qa'ida influenced radicalisation' (Bouhana and Wikström, 2011). At the same time, it should be acknowledged that the academic field in this area continues to develop: the study of terrorist groups' use of the internet has become an increasingly popular area. However, research has remained predominantly focused on websites and analyses of virtual communities (Bartlett 2012). A related area of growth in the academic field is the analysis of online content and its potential influence on vulnerable individuals. Notably, there has been little attention to the individual internet users' experience online and usage of the internet in the process of radicalisation, that is, whether and how the internet is associated with a person coming to support terrorism or forms of extremism leading to terrorism. When academic accounts do analyse these individuals' engagement with the internet, they often do so by examining secondary sources or anecdotal evidence. The largely and secondary and/or anecdotal basis of knowledge in this field points to a key gap in the academic research on radicalisation - namely access to and analysis of primary data on terrorist 'users' of the internet.

1.7. Re-balancing approaches to online radicalisation: insights from collected cases

The core argument of this study is that governments and the academic community have focused on the general *phenomenon* of the internet and radicalisation, rather than on a person's individual *experience*

online. Many of the public reports and studies look at the internet and attempt to describe how its messages and content are influencing people at risk of being radicalised. These studies describe the aims and evaluate the success of a particular terrorist or extremist group's online presence and media strategy. In short, they suggest a degree of causality between what is online and the influence on the person reading it, which cannot be proven. Additionally, the academic community's focus on content has meant that efforts have been concentrated on auditing a vast array of jihadist, extreme right-wing and single-issue protest websites that have appeared online. No doubt this provides policymakers and practitioners with insights into terrorists' narratives, marketing strategies, beliefs and organisation. These are all important factors, but this is only one side of the 'market' of online radicalisation, namely, the supply side of content. The demand side – how individuals choose to engage with material and interact online with like-minded individuals – remains a gap in policymaking and academic understanding.

The internet's role in the process of radicalisation has remained difficult to address. In spite of significant policy interest, action and academic work, little is known about individuals' experiences of the internet and their engagement with it during their radicalisation.

2. Methodology

This chapter outlines the methodological approach adopted by the research team. It first presents an overview of the methodology and its rationale. Secondly it explains the literature undertaken, and the subsequent gathering of primary evidence.

2.1. Overview of the approach

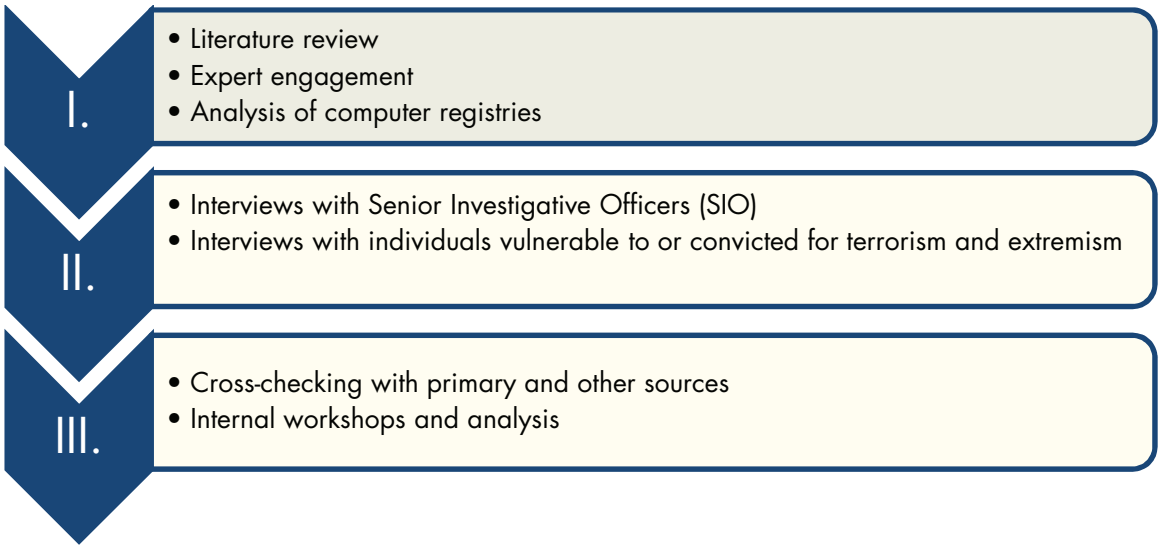
Given the complex and sensitive nature of the topic, unsurprisingly, there is a dearth of publicly available primary data available for analysis. The research team, however, gained access to first-hand accounts from radicalised individuals and terrorists as well as experts in counter-terrorism. The task then became one of understanding key arguments in the literature and assessing their fit or lack thereof, with the data we gathered. By focusing on collating primary data on the individual's experiences, we strived to probe key hypotheses derived from the literature and to outline insights of the patterns of individuals' online activity which may be useful to policymakers and practitioners.

Specifically, the study set out to ask the following questions:

- How is the internet used, if at all, in the individuals' process of radicalisation?
- In what way does a terrorist's or extremist's online activity relate to their actions offline?

The research team employed the following methodology: a literature review, a collection of primary data through semi-structured interviews, and an analysis of trial evidence including computer registries (where available). The methods used by RAND Europe in this study are introduced in Figure 3.

Figure 3: Stages of data collection



2.2. Literature review and stakeholder engagement

The project team first performed a literature review to identify key themes relating to internet radicalisation. This methodology consisted of a rigorous and systematic search and review of the literature, by determining specific search terms and defining exclusion/inclusion criteria. Initial literature was identified through a systematic search using a combination of search terms, including: a) radicalisation, extremism and terrorism, b) internet and online and c) role, effect, and influence. The research team identified further literature by snowballing from the initial literature.

The review focused on answering two related questions:

- What empirical evidence is available in the public domain on radicalisation and the role of the internet?
- What empirical evidence is available on terrorists' and extremists' use of the internet during their radicalisation process?

The research team used a number of internet resources in concert with a hand-search of relevant websites relating to radicalisation. We also obtained input from academics and policy experts within government to get an overview of the key issues and ideas currently informing policy. Such stakeholder engagement allowed the research team to best target the review of the literature through the identification of key documents, issues and challenges.

2.3. Primary data collection

A review of media reporting and other grey literature identified convictions of individuals for terrorist offences under UK Terrorist legislation (henceforth TACT) in which the use of the internet appeared to be an element of the offences, within the timeframe 2001-2012. Additionally, ACPO was approached and

briefed on the research aims and the cases identified as relevant. ACPO then identified, where possible, SIOs from British police forces who had led successful prosecutions[11] against the individuals we identified through the analysis of media reports. ACPO also suggested examples of cases which involved use of the internet in terrorist activities or where radicalisation through the internet was deemed to be an element of the case. Police forces further provided access to the cases of individuals who had not been prosecuted but were deemed to be vulnerable to the influence of extremists. These individuals were being engaged under the auspices of the Channel programme[12] – a component of the UK Government's Counter Terrorism strategy.

In some instances police forces with whom we engaged were able to facilitate access to the individuals who had been prosecuted or to suggest local intermediaries who could facilitate this access. Through this method of convenience sampling, the study gained access to primary data relating to 15 cases:

- Nine cases involved individuals convicted under the UK Terrorism legislation (TACT) (coded as A1-A2 and A4 to A10 in the report), one (A3) case related to a former member of an Islamist terrorist group; and
- Five cases of individuals were identified by the authorities as vulnerable (coded as B1 to B5 in the report).
- To probe key hypotheses in the literature and to understand and identify patterns of online radicalisation, the study explored through interviews or examination of trial records and first hand data;
- Individuals' level of radicalisation and involvement in violent extremism and/or terrorism - both in the real world and online;
- The personal circumstances and social relations of the individual who was being radicalised;
- The locations from which the individual used the internet, and for what purpose;
- The reasons why they used the internet instead of other forms of information and/or communications;
- Whether the individual's use of the internet changed over time and, if so, how; and
- Whether the internet helped to reinforce messages that the individual heard elsewhere.

An interview protocol and ethical framework was sent to all individuals before interviews took place (Government Social Research 2011). As with the literature review, the primary data collection was followed by a workshop to identify the key messages for each of the research questions.

[11] Successful prosecutions were identified because the subject of our analysis was convicted terrorists.

[12] The Channel programme, as described in the *Prevent* Strategy (2011), is a multi-agency approach to protect people at risk from radicalisation. Channel uses existing collaboration between local authorities, statutory partners (such as the education and health sectors, social services, children's and youth services and offender management services), the police and the local community to:

- identify individuals at risk of being drawn into terrorism;
- assess the nature and extent of that risk; and
- develop the most appropriate support plan for the individuals concerned.

2.4. Obstacles to data collection

A number of obstacles to using primary data stood in the way of understanding the internet's role in the process of radicalisation. The challenges encountered in designing and conducting research for this study are briefly set out below.

2.4.1. Limited access to primary data

Gathering new evidence of individuals' experiences of the internet is constrained by procedural, security and logistical barriers– not least for convicted terrorists and known extremists. Many of the convicted terrorists in our study are still serving their sentences. The researchers overcame this through engaging with ACPO - who provided us with otherwise inaccessible data from the individual cases.

2.4.2. Ethical constraints and data protection

There are significant ethical and data protection constraints to obtaining secondary information about known terrorists and extremists, for example from past investigations. For this reason, it is challenging to piece together an accurate picture of an individual's life and experiences. This challenge is compounded when the subject has been convicted of a crime and might volunteer only limited amounts of information, some of which may be deliberately misleading. The researchers mitigated the risk arising from this cluster of concerns by triangulating interviews wherever possible with data from trials and SIO perspectives.

2.4.3. Media-induced bias

Finally, some of the cases we highlight are well known and have been widely discussed in the media or involve evidence framed in a particular manner. This may introduce bias in how the cases are viewed by those undertaking the analysis and those reading it. As we discovered during the course of this project, the wider context (for example around individuals' behaviours, relationships or state of mind) of a particular case is rarely picked up outside of the police and security and intelligence agencies, despite the information being publically available. To address this, we coded the individual case studies to help neutralise any biases that the researchers or the reader may have regarding specific cases, and allow a more objective view. This approach had the following benefits: it ensured that the individuals interviewed were able to discuss openly their experiences and allowed the study to make use of information and data which could only be provided on a non-attributable basis.

3. Literature review: current understanding of the role of the internet in radicalisation

3.1. Introduction

The role of the internet in the process of radicalisation has generated widespread interest from policymakers, practitioners, academics and the media. Table 2 and Table 3 below illustrate the many results that Google yielded when searching for relevant phrases.

Table 2: Google search (July 2013) for keywords on internet radicalisation in English[13]

Search Term	Number of Results
"online radicalis(z)ation"	17,360
Out of that PDF files and reports	*711*
Results on Google Scholar	*197*
"internet radicalis(z)ation"	3,260
Out of that PDF files and reports	*355*
Results on Google Scholar	*83*

[13] In relevant cases, British and American spelling was used simultaneously to prevent any omissions, such as "radicalization" and "radicalisation".

Table 3: Google search (July 2013) for keywords on internet radicalisation in German and French

Search Term	Number of Results
"Radikalisierung durch das Internet" (German)	10,300
"Radicalisation sur Internet" (French)	18,500

However, the breadth of research does not always correlate with the depth of scholarship. The study examined more than 150 articles, of which only 18 were empirically derived studies.[14]

From our search the literature can be broadly categorised into four subject areas:

i. A focus on terrorist and extremist websites, with a plethora of studies on why groups use the internet (e.g. the aims of Al Qa'ida's media production house, as-Sahab;[15]
ii. Description of what is being posted on the internet, by analysing forum data or videos that terrorist groups upload to the internet;
iii. A focus on how individuals develop extremist ideas condoning violence and other illegal activity;
iv. An examination of how violent extremists and terrorists undertake operational research, planning and preparation for their attacks online.

3.2. Five themes emerging from the literature review

Most studies that were reviewed use language which ascribes a role to the internet in promoting radicalisation. The differing degree to which authors suggest the internet has a causal role in radicalisation is signified by the terms used in the literature, from 'facilitative' (broadening of opportunity) or 'reinforcing', to a more enhanced role as an 'accelerant' or the 'primary or sole driver' of radicalisation. The literature review culminated in an internal workshop to identify the key hypotheses from the literature. The following five were identified:

i. The internet creates more opportunities to become radicalised.

[14] Bermingham 2010, Chesser 2012, HoC Home Affairs Committee 2012, Torok undated, Wojcieszak 2010 and 2009, Warner 2010, Weimann 2008, de Koning 2011, Neumann 2010, Zeng 2011, Bowman-Grieve II, Caiani and Parenti. Dalgaard (PET Denmark) 2010, Gartenstein Ross (undated), AIVD 2010, Glithens-Mazer (undated)

[15] The As-Sahab Foundation for Islamic Media Publication (to give it its full title) relays Al Qa'ida's messages externally.

ii. The internet acts as an 'echo chamber'.
iii. The internet accelerates the process of radicalisation.
iv. The internet allows radicalisation to occur without physical contact.
v. The internet increases opportunities for self-radicalisation.

3.3. The internet creates more opportunities to become radicalised

3.3.1. The Internet helps facilitate radicalisation

Almost *all studies ascribe a role to the internet* in promoting radicalisation (cf. Precht 2008). Most studies suggest that the internet is a reinforcing agent or an accelerant, and has broken down the traditional barriers for individuals wanting to become radicalised (Pantucci 2011). A handful of studies suggest that the internet is a driver of radicalisation (Briggs and Strugnell 2009; Homeland Security Institute 2009).

A key text in the literature is Weimann's (2006) - which counts the number of websites of terrorist groups and reviews their content. In his widely-cited article, Weimann points to the proliferation of jihadist web sites: in 1998, fewer than half of the groups designated as foreign terrorist organisations by the US State Department maintained websites; by the end of 1999, nearly all these terrorist groups had established their presence online (2006).

However, there is *no clear attribution of causality* to the increasing number of web sites leading to an increase in radicalisation online. *At most a correlation* is suggested: for example, in Precht (2008):

> A recent empirical study of 242 European jihadists from 2001-2006, on the effects on the internet on radicalisation, found that there is a correlation between jihadi web sites and propaganda on the internet and rapid radicalisation.

3.3.2. The internet reaches otherwise unreachable individuals

The obstacles of geography and space in connecting individuals are reduced by the reach and immediacy of the internet. A number of studies point to the internet's ability to 'reach' those individuals who otherwise would not have been reachable by radicalisers in any other way (Neumann 2012). The success of Anwar al-Awlaki[16] in creating high-quality, high-production value content such as Inspire (Al Qa'ida's web magazine), which advocates 'jihad from home' and has been heavily distributed in the West, is cited as broadening the appeal of violent extremism (Quilliam 2010).

[16] Anwar al-Awlaki was a spokesperson and recruiter for Al Qa'ida.

3.3.3. The internet opens opportunities to radicalise a broader range of people

A handful of studies suggest that the internet has broken down some of the barriers that exist in the physical world for certain groups of people to become involved in extremism. This has been particularly highlighted in the case of women in relation to jihadism (Briggs and Strugnell, 2011); it may be unacceptable for women to meet in person with extremists who are men or to join their groups; it may also be unacceptable for them to express certain thoughts in public in the physical world. However, the internet affords them greater anonymity (Schmidle, 2009).

Some authors suggest that similar, self-imposed constraints may mean that shy individuals can benefit from the access that the internet gives them to radicalisation (Torok, 2010; Transnational Terrorism, Security & the Rule of Law, 2008; Yeap and Park, 2010). The reduction of signifiers of difference between individuals helps connect like-minded individuals from across the world, whatever their gender, background or country of residence. One person now disengaged from the extreme right-wing movement recounts how the internet 'was the easiest way to make contacts and to take over and coordinate responsibilities, to gain reputation and advance' (Köhler, 2012, p. 6). Bjelopera goes so far as to argue that:

> the interactivity [of the internet] blurs the lines between readership and authorship that previous generations of terrorists and sympathizers encountered with pamphlets, newspapers and newsletters. This blurring… encourages people… to more easily see themselves as part of broader jihadist movements and not just… [online spectators]. (2011, pp. 101–102)

3.4. The internet acts as an 'echo chamber'

Bjelopera (2011) highlights the internet's role as normalising behaviours and attitudes that otherwise may carry a risk of being considered unacceptable or inappropriate in the physical world. The internet provides supposed anonymity (Weimann, 2006) and a degree of protection and security from detection (Gray and Head, 2009). It also provides acceptance: information is non-censured and non-hierarchical (Bartlett, 2011). To give an illustrative example, an individual disengaged from the extreme right-wing movement communicated that 'some of them really run riot, placing swastikas wherever they can... because they think they are acting in a completely extrajudicial space' (Köhler, 2012 p.6).

The internet has been described as an 'echo chamber' (Ramakrishna, 2010; Saddiq, 2010; Stevens and Neumann, 2009) or a 'mental reinforcement activity' (Silber and Bhatt, 2007). The consensus in the literature is that the internet allows individuals to gain easier

access to the material in which they are interested, which is harder to do in the physical world where we more regularly come across individuals with different opinions or access material exposing different views (Briggs and Strugnell, 2011; Shetret, 2011). Moreover, the internet can give the illusion of 'strength in numbers', as Saddiq (2010) points out. As Schaan and Phillips explain, 'brought together by online journals, blogs, services and chat rooms, the participants enter forums where the extremist ideology becomes self-reinforcing' (2011, p. 24).

3.5. The internet accelerates the process of radicalisation

A feature which supports the notion of the internet as an accelerant in radicalisation is the fact that it offers a 'one-stop shop' for all the information that an extremist may seek out, or by which they may be influenced. As Stevens and Neumann explain:

> [T]he internet can be used by extremists to illustrate and reinforce ideological messages and/or narratives. Through the internet, potential recruits can gain... access to visually powerful video and imagery which appear to substantiate the extremists' political claims (2009, 12).

All of this can happen in a reduced timeframe compared to accessing the information in the 'real' (as opposed to virtual) world.

Many studies identify the internet as an accelerant of the radicalisation process, by virtue of the fact that it allows individuals to connect in an instantaneous and continuous way. This has led to the internet being referred to as a 'conveyor belt' (Bergin, 2009).

Pantucci highlights the internet's role in incubating (and accelerating) terrorism for some:

> [T]he internet is clearly the running theme between most of the plots included in this dataset and it appears to be a very effective tool: it provides a locus in which they can obtain radicalising material... It provides them with direct access to a community of like-minded individuals around the world with whom they can connect and in some cases can provide them with further instigation and direction to carry out activities (2011).

Schmidle (2009) points to the role of chat rooms in particular in this acceleration effect, as extremists can exchange with like-minded individuals 24/7, regardless of borders.

3.6. The internet allows radicalisation to occur without physical contact

As Yeap and Park explain, 'individuals have the comfort of accessing radical content from their own personal space instead of having to go through the inconvenience of physically

attending radical religious gatherings' (2010, p. 2). The internet therefore implies a much more limited set of logistical challenges to connecting with others: while the individual needs internet access, it is not necessary to make appointments and travel to other locations, for example.

While the internet may present fewer hurdles to interaction than physical meetings, the argument that radicalisation requires human interaction and physical proximity[17] fails to accept that we live in a digital era where our 'online' activities are an extension of our 'offline' lives. Friendship, personal relationships and loyalty are no longer the sole preserve of the physical world, but also exist virtually. Thus, some would argue, that radicalisation on the internet 'is not necessarily any different to what would happen with other more private and less visible sources' (Silber and Bhatt, 2007).

3.7. The internet increases opportunities for self-radicalisation

Some of the literature discusses the influential role of the internet in enhancing the likelihood of self-radicalisation. For some authors, self-radicalisation and radicalisation via the internet is one and the same thing. It refers to a process that is devoid of physical contact: the full process takes place online, and can include contact with others as long as it is remote (Change Institute, 2008; Homeland Security Institute, 2009). Bjelopera argues that 'internet activity has been central in the development of a "self-starter" phenomenon and offers would-be violent jihadists a "de-formalised" radicalization experience' (2011, p. 104). Al-Lami explains that this self-radicalisation essentially consists of 'individuals [becoming] familiar with and influenced by radical ideologies without even socialising with radical groups' (2009, p. 7). For others, the processes are different. What distinguishes self-radicalisation from radicalisation via the internet is that it takes place in isolation, and implies a process whereby no contact is made with other terrorists or extremists, whether in person or virtually. In this study, self-radicalisation is understood in this way.

The consensus is that self-radicalisation is extremely rare, if possible at all (Bermingham et al., 2009; Change Institute, 2008; Precht, 2008; Saddiq, 2010; Stevens and Neumann, 2009; Yasin, 2011). This is a challenging assumption to test, given that the available evidence may not point to relevant online or offline exchanges with other individuals, even if such exchanges exist or have occurred. However, there is evidence to suggest that in the large majority of cases, radicalisation does not occur solely through the internet, but instead involves offline contact. For example, the UK House of Commons Home Affairs Select Committee report 'Roots of Violent Radicalisation' (2012 p.65) confirms that 'even those witnesses who attributed a significant role to the internet tended to support that

[17] See House of Commons Home Affairs Select Committee, 2012.

report's conclusion that some element of face-to-face contact was generally essential to radicalisation taking place'.

3.8. Research on interactions between the online and offline worlds is rare

There is limited information on the way in which people's online and offline behaviours interact, which is a key area of focus in this study. From the 150 reports that were reviewed for the present study, only three studies dealt with the interplay of online and offline factors in radicalisation in an empirically robust manner. Wojcieszak (2010) examined the survey responses of neo-Nazi forum users; Warner (2010) examined how media of different ideological strains impact on students' political inclinations, while Neumann and Rogers (2007) drew on interviews from radicals,[18] former radicals and intelligence officials to describe the predominantly supporting role of individuals' online activity to a wider radicalisation processes.

3.9. Conclusions

This chapter has sought to provide a targeted overview of the current literature on the internet and radicalisation with a view to identifying key gaps to which this study can contribute. As Conway suggests:

> [T]here is an assumption that the internet plays a part in some individuals' radicalisation... but [there are] no large-scale studies showing this to actually be the case or measuring the extent of the internet's role in such processes. (Conway and McInerney, 2008, p.13)

Although the sample size of the present study is small, we intend to test the five hypotheses outlined above and explore two key issues in the coming chapters that warrant further consideration: a characterisation of how violent extremists' have used the internet during radicalisation, and the relationship between online and offline behaviour.

[18] Radicals or former radicals who were members of, or close to, groups or networks that approved of and/or facilitated violent extremism.

4. How 15 individuals engaged with the internet in their radicalisation: case studies and insights

This chapter explores the role of the internet in 15 cases of radicalisation through the data we were able to access. The chapter draws on information provided by interviews with the police and individuals, and maps these against the five hypotheses from the literature review. In a separate Annex we provide an overview of the individual cases as well as presenting data (such as computer registries) from trials where available. The aim is to provide the reader with a sense of what these individuals, the police and a review of trial documents suggested was relevant to the radicalisation processes in each case.

Box 1: Case studies breakdown

The 15 cases examined are broken down as follows:

- Nine of the cases are offenders convicted under the Terrorism Act 2000 or Terrorism Act 2006. These nine cases touch on both Islamist terrorism and the extreme right-wing.
- One case study is of a former member of Al Qa'ida who was active in Bosnia, Afghanistan and South-East Asia before disengaging from terrorist activities.
- Five of the cases were referred to the PREVENT intervention programme which tackles vulnerability (the Channel Programme).

4.1. Interview approach and objectives

In order to structure the interview process we set out specific lines of inquiry, while remaining open to the possibility of finding new information that was not expected. In designing the interview questions, we hoped to develop a picture of:

- The individual's background and the context in which they used the internet;
- The approximate age at which the individual began using the internet;
- The social arena preferred by the individual when spending time online;

- The purpose of the individual's time spent on the internet and whether they received guidance offline as to what this should be; and
- Whether the individual took substantial breaks from browsing online.

Following from this, we sought to begin understanding:

- The relationship between the internet and offline factors in the individual's radicalisation;
- The role of the internet at different stages of the individual's radicalisation process;
- The strengthening / reinforcing mechanism of the internet, if any; and
- The role the internet played in the individual's journey, if any.

4.2. Mapping our hypotheses against primary data findings

This section will further use the research findings to assess the validity of the five hypotheses made in chapter 3. Through an analysis of each individual's online and offline background, experience, attitudes and activities, this chapter aims to identify cross cutting themes and to better understand the role of the internet in the radicalisation process.

This section will map the five hypotheses themes from the literature review[19] against the findings drawn from our primary data (Annex A for further details). Table 4 provides a summary of how well our data fits with the conclusions drawn in the literature. These findings will be discussed in greater detail below, but it is worth noting that in some instances our findings have supported and in others they have challenged hypotheses made in the literature.

[19] See Chapter 3 for a detailed exploration of the five themes that emerged from the literature review.

Table 4: Mapping our hypotheses against primary data findings

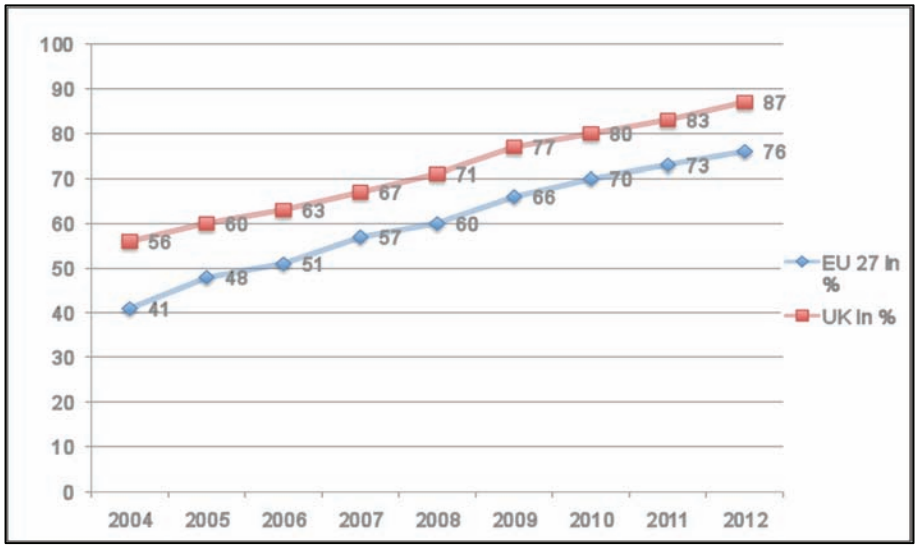
Literature hypotheses	Does the primary data support the hypotheses?
1. The internet creates more opportunities to become radicalised.	Yes in all of these cases
2. The internet acts as an 'echo chamber'.	Yes in the majority of these cases
3. The internet accelerates the process of radicalisation.	While there is no agreed length of time or template for radicalisation, it is not clear that the internet would have accelerated this process in the majority of our cases: in these cases the internet appears to enable rather than necessarily accelerate radicalisation
4. The internet allows radicalisation to occur without physical contact.	Not in the majority of these cases: most cases involve offline activity that could have played a role in the individual's radicalisation
5. The internet increases opportunities for self-radicalisation.	Not in the majority of these cases: most cases of so-called 'online self-radicalisation' involve virtual communication and interaction with others

4.2.1. The internet has created more opportunities to become radicalised

There is widespread evidence and support for the first hypothesis in the literature. In all of our 15 cases the internet provided the individual in question with a capability to connect, collaborate and convince. This is largely due to the now widespread use of the internet and increasing availability of extremist content online.

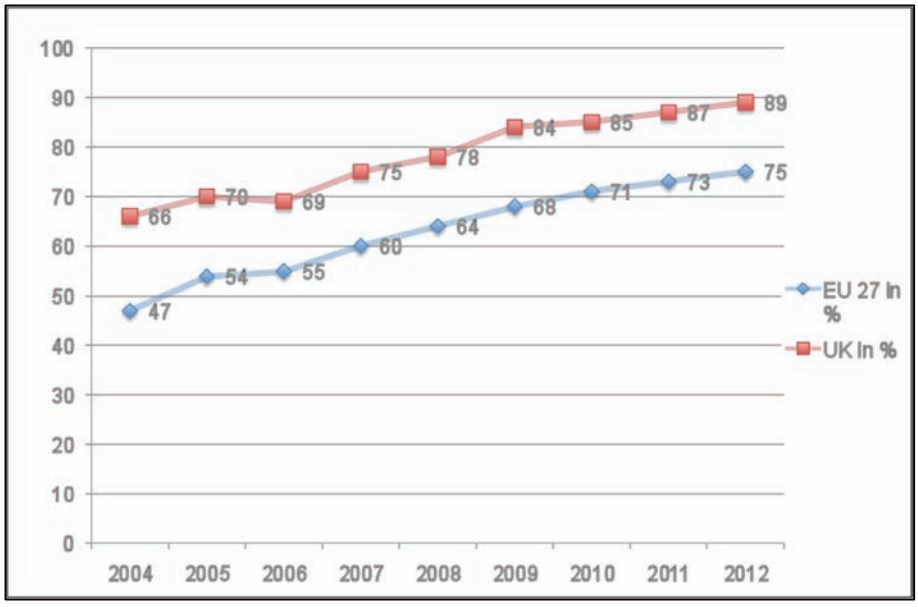
In the UK, internet access had reached penetration rates of 87% of households by 2012 (whilst the figure for the EU-27 at the time was a little lagging at 76%). Internet use among individuals stands at 89% in the UK and 75% for the EU. Figures 4 and5 show the growth in internet penetration and frequency of use for both the UK and the EU-27. This trend is matched, in turn, by a massive increase in the number of Jihadist websites now available – rising from 12 in 1998 to 4,500 by 2006 (ONS survey data, 2010).

Figure 4: Internet access in households in EU-27 and the UK (%)



Source: Eurostat 2013

Figure 5: Internet use amongst individuals in EU-27 and the UK (%)



Source: Eurostat 2012

In all 15 cases discussed in this report, the internet acted as a key source of information, a means of communication, and/or a platform for extremist propaganda. The internet appears, from these cases, to facilitate radicalisation. A1 and A2 used the internet to learn how bombs are made; A4 sought instructions on how to build suicide vests; B2 checked when and where EDL demonstrations would take place. For someone like A7, who grew

up in a socially conservative household which did not allow television, the internet became a viable medium for accessing knowledge and contacting people and positively fed into his radicalisation journey.

The internet enables connection with people who, due to potentially greater anonymity, may have lower thresholds for engaging in conversations that could be perceived as security risks. For A5, the perceived anonymity of the internet was a key factor and created the following opportunity:

> "the internet…(as a medium) allows those that would otherwise be scared of being seen with the wrong people to get engaged, and one which makes the whole process more invisible to the authorities. "

Even if some terrorists and/or extremists are skeptical of the internet's security they may, like A1 and A2, invest in encryption and deletion software to erase incriminating data instead of choosing not to use the internet at all.

The internet also opens opportunities for those seeking influence to radicalise a broader group of people. The lack of internet in the 1970s and 1980s meant that information on terrorism and extremism was found in books and/or VHS videos and cassette tapes. These needed to be identified, bought and circulated. The reach of the messages contained in these books or cassettes was limited. Contrast that limitation with the new reality illustrated in our cases: members of terrorist groups in Pakistan reached out to A10 to discuss military training whilst A7, A8 and A9 spread the word of the 'al Qa'ida cell' in the UK across the internet.

As described by A3, who grew up when VHS and cassettes were used to spread radicalised messages, the internet enables you to take your audience from "retail to wholesale levels". For B2, the dissemination capacity of the internet is very appealing:

> "The net was the best way of getting our messages further afield I think. It's better than all the leaflet runs the BNP used to do. Look how fast it is and how far it can get your stuff out – literally all over the world and no trudging around council estates putting leaflets through letterboxes and having dogs chasing after you! "

A3 shared with us an approximation of the widening pool for recruiters:

> "The internet is like a fishing net, catching surface fish, not bottom fish. We used to catch one at a time, now we catch 100-200 in a year."

As a former radicaliser, A3 made clear in his interview the benefits of the internet over other instruments. Before the spread of the internet he had to spend a lot of his time going from cafés to Chicken Cottage restaurants (a halal fast food chain), selling his ideas.

4.2.2. In most cases the internet acts as an 'echo chamber'

In Chapter 3 we learned that the internet allows individuals to seek material that they are interested in, and to reject that which does not support their worldview. The internet can give the illusion of strength of consensus in numbers and, as such, can act as a normalising agent (Bjelopera, 2011).

Several of our subjects helped to demonstrate this mechanism in operation. A1, A3, A5, A6, A10 and B2 all actively contributed to web forums that promoted the discussion of extremist topics. For B3, the intuitive strength of the internet is how it localises like-minded people, removing the sense "that it's just you with these feelings". In the offline world, we've already seen how A4 searched from mosque to mosque for a like-minded group, someone with whom to share his views. Having not found anyone, he took his search online.

A4 kept away from chat rooms, not willing to debate. His key word searches (see Annex A Figure A4) reveal that he went online primarily to gather information, rather than to engage.

A6, on the other hand, was willing to have his worldview tested. He welcomed debate online. If he found himself ignorant on a topic in a debate, he would go offline, learn more about that topic, and return to battle it out again. His online appearances dropped after such incidents, but he would return after a period of time (see the sometimes long gaps in A6's online activity in Annex A Figure A6).

On the whole, however, most of the information recovered by the police and shared with the research team suggests that the convicted terrorists examined in this study were not generally looking at information that may have challenged their extremist beliefs. It is, however, important to note that this finding may be due to the fact that the information recovered related to a late stage of the individual's radicalisation, or to the fact that they accessed this information from different profiles or computers. In fact, the police made clear that it is challenging to attribute information recovered from computers to individuals and to be confident that this information is representative of the individual's usage of the internet. 'Tech-savvy' individuals can use separate computers from different locations, they can hold multiple user names, break into others' profiles, or erase information from the computers they use.

4.2.3. The internet enables rather than accelerates the process of radicalisation

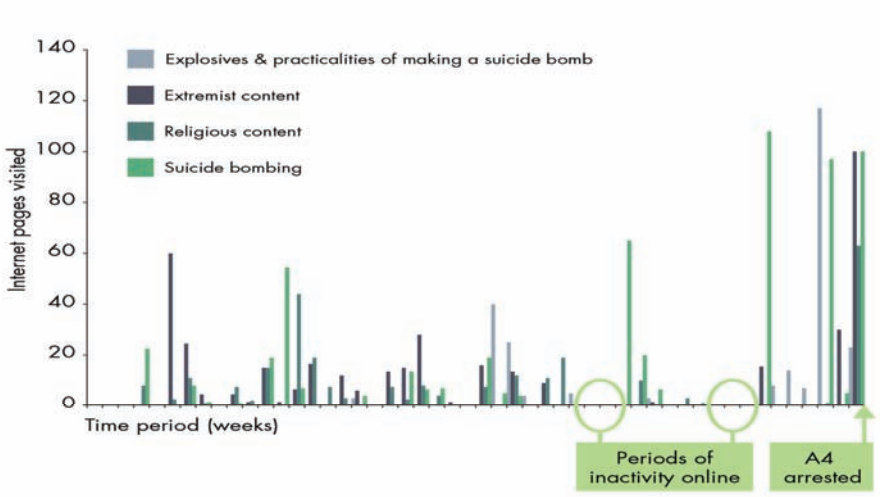
Based on the 15 cases above, it is hard to ascertain whether or not the internet accelerated the process of radicalisation. The relative significance of the internet as an accelerator, amongst all conceivable sources of radicalisation, is difficult to discern with such a small sample size and without fuller information on what else individuals might have been doing at the time and outside of their internet use. More factors would need to be considered before being able to provide a complete picture of all contributors to radicalisation.

The impact that seeing videos daily and having access to constant and immediate communication had on the *speed* of radicalisation for any of the individuals mentioned above is therefore not clear from the narratives. As noted by A3, the experience of each individual online is inherently subjective: while the internet might make information easier to find, the impact of doing so may differ from individual to individual.

For the majority of our cases, the internet appeared to *facilitate* the process (explained in some detail in 4.3.1 above), and this in turn may or may not accelerate it.

In the case of A1 and A2, it is likely that the process of radicalisation built over a number of years. A5 eventually rejected the internet as a path to radicalisation (in his interview he expressed dismay at the infighting that took place in chat rooms, and how this drove him offline). A4's experience also indicates that the internet did not necessarily accelerate his radicalisation process. As shown in Figure 6 below, his periods of inactivity online before his arrest indicate that external factors may have accelerated his radicalisation as much as or more than his online activity.

Figure 6: A4's timeline leading to arrest



4.2.4. Most cases involve offline activity that could have played a role in the individual's radicalisation

The case study evidence suggests that online and offline factors both play an important and interconnected role in the radicalisation process. From the case summaries above, it appears likely that there is an iterative process through which events and developments in the physical world feed into online behaviour and vice versa. This evidence suggests that the internet is not a substitute for but rather complements in-person communication.

Before the convictions of A1 and A2, newspapers reported that their radicalisation exclusively took place online. Although a review of their online activities does show that A1 and A2 downloaded extremist material, even from the small picture above we can appreciate the more nuanced interaction with, and likely effect of, personal relationships. A2, we have seen, was influenced in her radicalisation by A1. A1 was active offline – he attended a conference and received a disc with extremist content. A personal relationship was also prevalent in the case of A5 who claimed the motive of growing closer to his dad, who was active on extreme websites, for his move towards online radicalisation.

Our research also showed that offline factors can sometimes be more influential than online factors in the radicalisation process. A10 was, for instance, first approached by a terrorist facilitator from Pakistan at the central mosque in Dewsbury. This meeting pointed A10 to search for online information on bomb-making and other extremist material. Following their introduction at the mosque, A10 and the facilitator began to communicate regularly online, where A10 was 'groomed' for a UK mission. This case suggests that the internet was primarily a resource for information, rather than the focus of A10's radicalisation. Similarly, A6's path to radicalisation, and affiliation with al-Mujahiroun, began with a physical meeting during a march in front of the US embassy. A3 was radicalised in Bosnia in the 1990s (before the advent of widespread internet use).

4.2.5. Most cases of so-called 'online self-radicalisation' involve virtual communication and interaction with others

On the whole, we have seen very little evidence to support the existence of any 'self-starters' in our cases. Amongst those in law enforcement and policymaking circles, the notion of 'self-radicalisation' appears largely defunct. To help illustrate this point, it is helpful to consider the UK's definition of radicalisation as found in the *Prevent* strategy:

> (Radicalisation is) a social process particularly prevalent in small groups. Radicalisation is about 'who you know'. Group bonding, peer pressure and indoctrination are necessary to encourage the view that violence is a legitimate response to perceived injustice. (UK Home Office, 2011)

Any suggestion of self-radicalisation is avoided. The case of Roshana Choudhry, mentioned earlier in the report, is seen by experts as an outlier. The Crown Prosecution Service has reviewed the case several times in order to understand whether she had links to known terrorist or extremist networks. It is considered that she remains one of a small number of cases where so-called 'self-radicalisation' via the internet took place.

The majority of the cases that we reviewed during our research, however, involved virtual and/or physical contact between individuals. For category A case studies, the trail of online and offline interactions is fairly clear. A1, for instance, used five Facebook accounts to engage with other extremists online; A3 was surrounded by extremists from a young age; A5 followed his father into extremism; A6 and A10 were targeted by terrorist facilitators while A7, A8 and A9 had a radicalising effect on one another.

5. Recommendations and conclusions

Tackling terrorism and violent radicalisation have been priorities for the European Union (EU) and its Member States following the US, Madrid and London bombings in 2001, 2004 and 2005 respectively. Initially, the concern was mainly with Islamist radicalisation but within a decade, and most notably as a result of Breivik's coordinated attacks in Norway, the perspective on the threat posed by radicalisation has once again widened to include the more traditional threats of right- and left-wing extremists, and nationalist-separatists. The Boston bombings in 2013 acted as a reminder to the policy world and the public that the threat of terrorism is ongoing, and re-emphasised the importance of research and policy action in the field of internet radicalisation[20]. As noted earlier in this report, on the whole, terrorism cases in the UK and the rest of Europe without a digital footprint are increasingly rare.

However, the internet is obviously only one part of the whole picture of radicalisation and terrorism; it is important not to amplify its significance. If the internet can have a radicalising effect, then it is but one of several plausible sources of radicalisation, including schools, faith-based organisations, prisons, work-place environments and even families and friends. It remains to be established what is its relative significance.

This chapter takes the findings and insights from the current study to develop recommendations for further research and policy action.

5.1. The importance of primary data for further research

The internet offers terrorists and extremists increased capability to communicate, collaborate and convince others to join in their beliefs. In recent years, practitioners and the academic community have begun to examine how the internet influences the process of radicalisation; how a person comes to support terrorism and forms of extremism leading to terrorism. The majority of policy documents and academic literature reviewed for this study predominantly focus on online content and its potential influence on vulnerable

[20] The Tsarnaev brothers, it is reported, were influenced to a big extent via Jihadist websites.

individuals, rather than exploring how individuals use the internet in the process of radicalisation.

The analysis of the supply side of radicalisation (what is offered by the medium) seems to be over-represented in the academic research, whereas the demand side remains neglected. The reason for this is relatively straightforward: access to terrorists (those convicted under UK terrorism legislation) or extremists (identified by the police and multi-agency partners based on a risk assessment) willing to speak to researchers is extremely difficult. Access to primary data understandably remains a significant challenge. However, such access is possible, as this study demonstrates.

A more sophisticated strategy that also targets individuals rather than solely focusing on the supply side, i.e. the medium, will require more research, but is an approach that is likely pay great dividends, providing a more accurate picture in the long term. Rather than using an either-or approach, it is hence essential for further research to find the right balance between both aspects.

The results from this work were based on a small number of cases and we cannot claim that they are representative of the wider terrorist population; they do not necessarily reflect the way in which other violent extremists and terrorists use the internet during their radicalisation. However, even this small number of cases has provided information with which it has been possible to test, validate and challenge some of the suggestions drawn from the literature to date in this field. In doing so, our study demonstrates the importance of gathering empirical evidence when seeking to explore a complex phenomenon such as online radicalisation. This analysis could therefore serve as a useful starting point for further research in the domain of online radicalisation.

5.2. The internet as a mode, rather than a single method of radicalisation - mapping literature hypotheses against real cases

The primary evidence from this study confirmed that for all 15 individuals we researched, the internet had been a key source of information, of communication and of propaganda for their extremist beliefs. The internet may furthermore enhance opportunities to become radicalised, as a result of being accessible to a large and growing number of people irrespective of gender or ethnicity, and enabling them to connect with like-minded individuals from across the world. This access to people online may provide greater opportunity than the offline world to confirm existing beliefs and avoid confrontation with information that would challenge these. The hypothesis that the internet works as an echo chamber can therefore be supported by this study.

However, the hypothesis that the internet allows radicalisation without physical contact cannot be supported. In all our cases the so called offline world played an important role in the radicalisation process. The subjects had offline contact with family members or friends who shared their beliefs. The internet is therefore not replacing the need for individuals to meet in person during their radicalisation. The same argument is true for the process of self-radicalisation which could not be supported by our cases and according to our research is more an exceptional phenomenon than the rule.

From this study it appears that it would be useful to analyse the interplay between the off- and online world. That an individual possesses a USB stick with extremist material, has Facebook accounts exhorting violent jihad, or has watched beheading videos is not necessarily evidence of 'radicalisation' or 'online radicalisation'. Rather, it suggests that a wider investigation of the individual is necessary in order to understand why they have acquired, posted or watched such material in the first place. This evidence, and the role of the internet in their radicalisation, must be placed within the broader context of the individual's personal history and social relations.

One of our overall conclusions therefore is that the internet has to be seen as a mode, rather than a unitary method, of radicalisation (the internet can play an important role in *facilitating* the radicalisation process; however, it cannot drive it on its own). Instead, the internet appears to enhance the process, which, in turn, may or may not accelerate it.

5.3. Framing possible policy responses

For practitioners, the increasing reach of the internet (from laptops to smartphones and tablets) raises numerous challenges. Based on interviews with police, security and intelligence officials, the authors' judgement is that relevant agencies will need to re-assess the thresholds and criteria for investigation and intervention, as opportunities to access and engage with extremist material increase. This need poses a number of issues, not least whether relevant agencies have the appropriate resources.

5.3.1. Differing approaches and regulatory environment

Given the challenges they face in this field, governments are likely to benefit from taking a range of approaches. Counter-radicalisation programmes implemented in Western countries differ greatly from one another, and from non-Western programmes, in terms of aims, structure, budget, and underlying philosophy. Each national experience is shaped by the political, cultural, and legal elements unique to that country (Vidinio & Brandon 2012, p. 7).

The United Nations Office on Drugs and Crime (2012) report on this subject outlines the challenge governments face when attempting to tackle terrorism-related content on the

internet. Approaches vary, with some states applying strict regulatory controls on Internet Service Providers (ISPs) and other related service providers, including in some cases the use of technology to filter or block access to certain content. Other states adopt a lighter regulatory approach, relying to a greater extent on self-regulation by the information sector. Most ISPs, web hosting companies, file-sharing sites and social networking sites have terms of service agreements that prohibit certain content; some terrorism-related content might contravene these contractual restrictions.[21]

5.3.2. Investing in people

It is widely agreed by the people interviewed for this study that the use of the internet by terrorists and extremists is a critical issue for the police and other agencies, and responding to this challenge will require greater investment in people and resources. In order to do so the police and government authorities will need to invest more in their digital literacy skills in the long run. The senior officers interviewed for this project are aware that they require more training and resources for tackling online crime, including terrorism and extremism. They all believe that as technology and threats evolve, so too will the need for further investment in training and equipment. Education and training should have two aims: to increase the digital awareness and to improve the digital resilience of supporting institutions.

5.3.3. Identifying red-flags

The police and relevant agencies might require closer relationships in the future with companies such as Facebook and Google to assist them in identifying red flags for vulnerable individuals. For example, in one of our case studies, A1 created Facebook accounts which Facebook closed due to their inappropriate use of beheading videos. However, this was never followed up with UK police forces, and A1 opened other Facebook accounts with similar identities (the identities were sequential: the last digit of the new identity would differ by one). Facebook did not go a step further than what was strictly necessary to identify or flag this pattern with the police.

Therefore, a more collaborative and innovative relationship between Internet Service Providers (ISP's), social media companies and the police might be essential. However, what needs to be clear as well is that ISP's are not watchdogs in the service of the governments. What is required instead is an effective collaboration between the police forces and ISPs to prioritise, as well as detect and tackle online extremist activity. It remains to be seen how interested ISPs are in working in close collaboration with police forces and governments.

---

[21] See the EU's Clean IT Project: http://www.cleanitproject.eu/.

5.3.4. Bridging ethical concerns

In a policy debate on the role of the internet governments should reflect on some of the ethical dilemmas as well as the operative ones – when to intervene and how to balance security and civil liberties. While it is the duty of governments to protect their citizens from terrorism, people's privacy needs to equally be protected to the fullest extent possible. Digital technologies have become an integral component of modern day life. Governments must be aware of the thin line between observing the web for security purposes and the creation of a 'surveillance society'. Recent events in 2013, where a whistle-blower revealed activities of secret services (i.e. NSA) wiretapping citizens, demonstrate the fragility of this thin line. Government action must therefore tread carefully around this line and find a balance between the security of the population as a whole and for those who might be subject to surveillance. If care is not taken in working at this interface of surveillance and privacy, then the privacy of most citizens, who are not affiliated with radical ideas becomes at risk. The danger of becoming too visible for governments and/or private companies should hence be taken into consideration when thinking of new approaches to protect the internet from the spread of radical ideas.

5.3.5. Forming an effective and appropriate counter-narrative

Hundreds of millions of euros have been invested in counter-terrorism policies and interventions. Yet more than 12 years after the September 11 attacks, there is widespread recognition that governments still find it challenging to measure the effectiveness of their counter terrorism work and to learn from it.[22] With respect to the internet and radicalisation, policymakers will have to adopt increasingly innovative methods to disrupt, take down and/or filter unwanted content. One part of such a continuous approach is to evaluate past and present activities in this area as in others.

The British government has undertaken some evaluation of its counter-narrative work online; however, for legitimate reasons it has not made this work public, as doing so could damage any gains made, especially those gains that have supported civil society groups. That said, the absence of a robust, comprehensive evaluation of counter-narrative work online is a concern – not least because it is not clear whether the work is well targeted or effective in changing the attitudes or behaviours of those vulnerable individuals engaging with radicalising material online. Unlike recent reports that have called for more counter-narrative work, the authors believe that independent assessment of the many counter-narrative projects would be beneficial to inform and help guide future activity.

[22] See official and scientific documents: European Commission's Expert Group on Violent Radicalisation (2008); Reding, A. *et al.* (2011); Rabasa, A. *et al.* (2010); Disley, E. *et al.* (2010); Horgan, J. and K. Braddock (2010)

References

Al-Lami, Mina, 'Studies of Radicalisation: State of the Field Report'. Politics and International Relations Working Paper Series, No. 11, London: University of London, 2009.

Audiovisual Media Services (AMS) Directive. 2010. 2010/13/EU. As of 04/09/2013: http://europa.eu/legislation_summaries/audiovisual_and_media/am0005_en.htm

Bergin, Anthony, 'Countering Online Radicalisation in Australia'. Australian Strategic Policy Institute Forum, 2009. As of 18 October 2012: http://www.aspi.org.au/research/spf.aspx?tid=9

Bermingham, Adam, Maura Conway, Lisa McInerney, Neil O'Hare and Alan F. Smeaton, 'Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation'. Paper presented at the Advances in Social Networks Analysis and Mining Conference, Athens, Greece, 20–22 July, 2009.

Bjelopera, Jerome P., 'American Jihadist Terrorism: Combating a Complex Threat'. Congressional Research Service Report for Congress, Washington, DC: Congress Research Service, 2011.

Bouhana, Noémie and Per-Olof H. Wikström, 'Al Qa'ida-Influenced Radicalisation: A Rapid Evidence Assessment Guided by Situational Action Theory'. Research, Development and Statistics, London: Home Office, 2011. As of 25 January 2013: http://www.homeoffice.gov.uk/publications/science-research-statistics/research-statistics/counter-terrorism-statistics/occ97?view=Binary

Briggs, Rachel and Alex Strugnell, 'Radicalisation: The Role of the Internet'. Policy Planners' Network Working Paper, London: Institute for Strategic Dialogue, 2011.

Castells, Manuel and Gustavo Cardoso, eds, *The Network Society: From Knowledge to Policy*, Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005.

Change Institute, 'Studies into Violent Radicalisation: Lot 2 – The Beliefs Ideologies and Narratives', 2008. As of 18 October 2012: http://ec.europa.eu/home-

affairs/doc_centre/terrorism/docs/ec_radicalisation_study_on_ideology_and_narrative_en.pdf

Conway, Maura and Lisa McInerney, 'Jihadi Video and Auto-Radicalisation: Evidence from an Exploratory YouTube Study'. In: Ortiz-Arroyo, Daniel, Henrik Legind Larsen, Daniel Dajun Zeng, David Hicks and Gerhard Wagner, eds, *Intelligence and Security Informatics: First European Conference, EuroISI 2008: Esbjerg, Denmark, December 2008 – Proceedings*, Berlin: Springer, 2008, pp.108–118.

Council of the European Union. 2002. Council Framework Decision of 13 June 2002 on combating terrorism. 2002/475/JHA. As of 04/09/2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0475:EN:HTML

Council of the European Union. 2005a. The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism. 14781/1/05, Brussels: European Commission

Council of the European Union, 2005b. The European Union Counter-Terrorism Strategy

European Commission. 2006. Communication: "Terrorist Recruitment – Addressing the factors contributing to violent radicalization". Brussels: European Commission.

Europol. 2013. TE-SAT 2013: EU Terrorism Situation and Trend Report. European Police Office, 2013. As of 3/09/2013: https://www.europol.europa.eu/sites/default/files/publications/europol_te-sat2013_lr_0.pdf

Government Social Research, 'GSR Ethics Checklist', UK Civil Service, nd. As of 2 August 2012:http://www.civilservice.gov.uk/wp-content/uploads/2011/09/gsr_ethics_checklist_tcm6-7326.pdf

Gray, David H. and Albon Head, 'The Importance of the Internet to the Post-modern Terrorist and its Role as a Form of Safe Haven'. *European Journal of Scientific Research*, Vol. 25, No. 3, 2009, pp.396–404.

Homeland Security Institute, 'The Internet as a Terrorist Tool for Recruitment and Radicalisation of Youth', 24 April 2009. As of 5 January 2013: http://www.homelandsecurity.org/docs/reports/Internet_Radicalization.pdf

House of Commons Home Affairs Committee, 'Roots of Violent Radicalisation', Nineteenth Report of Session 2010–12, Vol. 1, 2012. As of 10 January 2013: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1446/144605.htm

Huffington Post. 2010. 'YouTube Gives Users Ability To Flag Content That Promotes Terrorism'. As of 03/09/2013: http://www.huffingtonpost.com/2010/12/13/youtube-terrorism-flag_n_796128.html

Jenkins, Brian, 'Stray Dogs and Virtual Armies: Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11', RAND Corporation, 2011. As of 18 October 2012: http://www.rand.org/pubs/occasional_papers/OP343.html

Köhler, Daniel, 'Internet and Radicalizations: Connecting the Dots – The Role of the Internet in the Individual Radicalization Processes of Right-wing Extremists'. Working Paper Series, Berlin: Institute for the Study of Radical Movements, 2012.

Laville, Sandra, 'Unpredictable "Lone Wolves" Pose Biggest Olympic Security Threat'. *The Guardian*, 9 March 2012. As of 22 October 2012: http://www.guardian.co.uk/uk/2012/mar/09/lone-wolves-olympic-security-threat

Neumann, Peter R., 'Options and Strategies for Countering Online Radicalization in the United States', Studies in Conflict & Terrorism, 2013. As of 23 September 2013: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2013.784568#.UkAWYNKnp0I

Neumann, Peter R. and Brooke Rogers, *Recruitment and Mobilisation for the Islamist Militant Movement in Europe*, London: International Centre for the Study of Radicalisation and Political Violence, King's College London, 2007.

Pantucci, Raffaello, 'A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists'. Developments in Radicalisation and Political Violence, International Centre for the Study of Radicalisation and Political Violence, 2011. As of 20 January 2013: http://icsr.info/2011/04/a-typology-of-lone-wolves-preliminary-analysis-of-lone-islamist-terrorists/

Precht, Tomas, Homegrown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism. An Assessment of the Factors Influencing Violent Islamist Extremism and Suggestions for Counter Radicalisation Measures, Copenhagen: Danish Ministry of Defence, 2008. As of 10 February 2013: http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/2011/2007/Home_grown_terrorism_and_Islamist_radicalisation_in_Europe_-_an_assessment_of_influencing_factors__2_.pdf

Radicalisation Awareness Network. 2012. *Proposed Policy Recommendations for the High Level Conference*, 2012.

Radicalisation Awareness Network (RAN). 2013. Update 7. As of 04/09/2013: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/ran-news/docs/ran_update_7_en.pdf

Ramakrishna, Kumar, 'Self-radicalisation and the Awlaki Connection'. S. Rajaratnam *School of International Studies*, 2010. As of 18 October 2012: http://dr.ntu.edu.sg/bitstream/handle/10220/6622/RSIS0752010.pdf?sequence=1

Ryan, Johnny, 'Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web'. *Institute of European Affairs*, 2007.

Saddiq, Mohamed Abdul, 'Whither e-Jihad: Evaluating the Threat of internet Radicalisation'. S. Rajaratnam School of International Studies, 2010. As of 18 October 2012: http://dr.ntu.edu.sg/bitstream/handle/10220/6646/RSIS0832010.pdf?sequence=1

Schaan, Joan Neuhaus and Jessica Phillips, *Analyzing the Islamic Extremist Phenomenon in the United States: A Study of Recent Activity*, Houston, TX: James A. Baker III Institute for Public Policy, Rice University, 2011.

Schmidle, Robert E., 'Positioning Theory and Terrorist Networks'. *Journal for the Theory of Social Behaviour*, Vol. 40, No. 1, 2009, pp.65–78.

Shetret, Liat, *Use of the Internet for Counter-terrorist Purposes*, Washington, DC: Center on Global Counterterrorism Cooperation, 2011.

Silber, Mitchell D. and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York: New York City Police Department, 2007. As of 16 October 2012: http://www.nypdshield.org/public/SiteFiles/documents/NYPD_Report-Radicalization_in_the_West.pdf

Stevens, Tim and Peter R. Neumann, *Countering Online Radicalisation: A Strategy for Action*, London: International Centre for the Study of Radicalisation and Political Violence, 2009.

Torok, Robyn, 'Make a Bomb in Your Mums Kitchen': Cyber Recruiting and Socialisation of "White Moors" and Home Grown Jihadists'. Edith Cowan University Research Online, 2010. As of 18 October 2012: http://ro.ecu.edu.au/act/6/

Transnational Terrorism, Security & the Rule of Law, 'Causal Factors of Radicalisation', 1 April 2008. As of 18 October 2012: http://www.transnationalterrorism.eu/tekst/publications/Causal%20Factors.pdf

UK Home Office, 'Countering International Terrorism: The United Kingdom's Strategy', Cm 6888, July 2006. As of 22 October 2012: http://www.official-documents.gov.uk/document/cm68/6888/6888.pdf

UK Home Office, 'Pursue Prevent Protect Prepare: The United Kingdom's Strategy for Countering International Terrorism', Cm 7547, March 2009. As of 22 October 2012: http://www.official-documents.gov.uk/document/cm75/7547/7547.pdf

UK Home Office, 'Prevent Strategy', 2011. As of 22 October 2012: http://www.homeoffice.gov.uk/publications/counter-terrorism/prevent/prevent-strategy/

United Nations Office on Drugs and Crime, 'The Use of the Internet For Terrorist Purposes', September 2012.

US Senate Committee on Homeland Security and Governmental Affairs, *Zachary Chesser: A Case Study in Online Islamist Radicalization and its Meaning for the Threat of Homegrown Terrorism*, Washington, DC: United States Senate, 2012.

Walker, Jesse, 'The Facebook Friend in the Plastic Bubble: Are We Filtering Ourselves to Death?' *Reason*, 14 July 2011. As of 22 October 2012: http://reason.com/archives/2011/07/14/the-facebook-friend-in-the-pla

Warner, Benjamin R., 'Segmenting the Electorate: The Effects of Exposure to Political Extremism Online', *Communication Studies*, Vol. 61, No. 4, 2010, pp.430–444.

Weimann, Gabriel, *Terror on the Internet: The New Arena, The New Challenges*, Washington, DC: United States Institute of Peace Press, 2006.

Wojcieszak, Magdalena, '"Don't Talk to Me": Effects of Ideologically Homogeneous Online Groups and Politically Dissimilar Offline Ties on Extremism'. *New Media & Society*, Vol. 12, No. 4, 2010, pp.637–655.

Yasin, Nur Azlin Mohamed, 'Online Indonesian Islamist Extremism: A Gold Mine of Information'. S. Rajaratnam School of International Studies, 2011. As of 18 October 2012: http://dr.ntu.edu.sg/bitstream/handle/10220/7889/RSIS1442011.pdf?sequence=1

Yeap, Su Yin and Jenna Park, 'Countering Internet Radicalisation: A Holistic Approach'. S. Rajaratnam School of International Studies, 2010. As of 18 October 2012: http://dr.ntu.edu.sg/bitstream/handle/10220/6657/RSIS0782010.pdf?sequence=1

Selected bibliography

Aly, Anne, 'The Internet as Ideological Battleground'. Edith Cowan University Research Online, 2010. As of 18 October 2012: http://ro.ecu.edu.au/act/9

Awan, Akil N., 'Radicalization on the Internet? *THE RUSI Journal*, Vol. 152, No. 3, 2007a, pp.76–81.

Awan, Akil N., 'Virtual Jihadist Media: Function, Legitimacy and Radicalizing Efficacy'. *European Journal of Cultural Studies*, Vol. 10, No. 3, 2007b, pp.389–408.

Bergin, Anthony, Sulastri Bte Osman, Carl Ungerer and Nur Azlin Mohamad Yasin, 'Countering Internet Radicalisation in Southeast Asia'. Australian Strategic Policy Institute Special Report, Issue 22, Canberra: Australian Strategic Policy Institute, 2009.

Booth, William, 'Doctor Killed During Abortion Protest'. *Washington Post*, 11 March 1993. As of 22 October 2012: http://www.washingtonpost.com/wp-srv/national/longterm/abortviolence/stories/gunn.htm

Borum, Randy, 'Radicalization into Violent Extremism I: A Review of Social Science Theories'. *Journal of Strategic Security,* Vol. 4, No. 4, 2011a, pp.7–36.

Borum, Randy, 'Radicalization into Violent Extremism II: A Review of Social Science Theories'. *Journal of Strategic Security,* Vol. 4, No. 4, 2011b, pp.37–62.

Bott, Catherine, James W. Castan, Robertson Dickens, Thomas Rowley, Erik Smith, Rosemary Lark and George Thompson, *Recruitment and Radicalization of School-Aged Youth by International Terrorist Groups*, Washington, DC: Homeland Security Institute, 2009a.

Bott, Catherine, James W. Castan, Robertson Dickens, Thomas Rowley, Erik Smith, Rosemary Lark and George Thompson, *The Internet as a Terrorist Tool for Recruitment and Radicalization of Youth*, white paper, Washington, DC: Homeland Security Institute, 2009b.

Bowman-Grieve, Lorraine, 'Exploring "Stormfront": A Virtual Community of the Radical Right'. *Studies in Conflict and Terrorism*, Vol. 32, No. 11, 2009, pp. 989–1007.

Bowman-Grieve, Lorraine. 'A Psychological Perspective On Virtual Communities Supporting Terrorist and Extremist Ideologies as a Tool for Recruitment'. Paper presented at the European Intelligence and Security Informatics Conference, IEEE Computer Society, Athens, Greece, 12–14 September 2011.

Briggs, Rachel and Jonathan Birdwell, 'Radicalisation among Muslims in the UK'. Policy Working Paper 7, London: MICROCON, 2009.

Brunst, Phillip W., 'Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet'. In: Wade, Marianne and Almir Maljević, eds, *A War on Terror? A European Stance on a New Threat, Changing Laws and Human Rights Implications*, New York: Springer, 2010, pp.51–76.

Caiani, Manuela and Linda Parenti, 'The Dark Side of the Web: Italian Right-wing Extremist Groups and the Internet', *South European Society and Politics*, Vol. 14, No. 3, 2011, pp.273–294.

Canadian Centre for Intelligence and Security Studies, *Militant Jihadism: Radicalization, Conversion, Recruitment*, Ottawa: Norman Paterson School of International Affairs, Carleton University, 2006.

Charvat, Julian, 'Radicalization on the Internet'. In: Iklódy, Gábor, Jaak Aaviksoo, Alan E. Brill, Marco Gercke, Anna-Maria Talihärm and Julian Charvat, 'Defence Against Terrorism Review', *Defence Against Terrorism*, Vol. 3, No. 2, 2010, pp.75–86.

Chen, Hsinchun, 'Sentiment and Affect Analysis of Dark Web Forums: Measuring Radicalization on the Internet'. Paper presented at the IEEE Intelligence and Security Informatics Conference, Taipei, Taiwan, 17–20 June 2008.

Chen, Hsinchun, 'Dark Web: Exploring and Mining the Dark Side of the Web'. Paper presented at the IEEE European Intelligence and Security Informatics Conference, Athens, Greece, 12–14 September 2011.

Cilluffo, Frank J., Sharon L. Cardash and Andrew J. Whitehead, 'Radicalization: Behind Bars and Beyond Borders'. *Brown Journal of World Affairs*, Vol. 13, No. 2, 2007a, pp.113–122.

Cilluffo, Frank, Gregory Saathoff, Jan Lane, Sharon Cardash and Andrew Whitehead, *NETworked Radicalization: A Counter-Strategy*, Washington, DC: Homeland Security Policy Institute and Critical Incident Analysis Group, 2007b.

Claiborne, William, 'Two Killed at Clinic in Florida'. *Washington Post*, 30 July 1994. As of 22 October 2012: http://www.washingtonpost.com/wp-srv/national/longterm/abortviolence/stories/florida.htm

Clarkson, Frederick, 'Anti-abortion Bombings Related'. Intelligence Report, Issue 91, Southern Poverty Law Center, 1998.

Co-Chairmen, 'Implementing the UN General Assembly's Counter-Terrorism Strategy: Addressing Youth Radicalisation in the Mediterranean Region: Lessons Learned, Best Practices and Recommendations'. Paper presented at the Istituto Affari Internazionali, Rome, 11–12 July 2007.

Commission's Expert Group on European Violent Radicalisation, 2008, 'Radicalisation Processes Leading to Acts of Terrorism', Report Submitted to the European Commission

Conway, Maura, Terrorism and the Internet: New Media – New Threat?' *Parliamentary Affairs*, Vol. 59, No. 2, 2006, pp.283–298.

Conway, Maura, 'From al-Zarqawi to al-Awlaki: The Emergence of the Internet as a New Form of Violent Radical Milieu', 2012. As of 18 October 2012: http://www.isodarco.it/courses/andalo12/doc/Zarqawi%20to%20Awlaki_V2.pdf

Cornish, Paul, *Terrorism, Radicalisation and the Internet: Report of a Private Roundtable Discussion on 22 July 2008*, London: Chatham House, 2008.

Dalgaard-Nielsen, Anja, 'Violent Radicalization in Europe: What We Know and What We Do Not Know'. *Studies in Conflict and Terrorism*, Vol. 33, No. 9, 2010, pp.797–814.

Daly, Christopher B., 'Salvi is Convicted of Murder in Abortion Clinic Shootings'. *Washington Post*, 19 March 1996. As of 22 October 2012: http://www.washingtonpost.com/wp-srv/local/longterm/aron/salvi021996.htm

De Koning, Martijn, 'Identity in Transition: Connecting Online and Offline Internet Practices of Moroccan-Dutch Muslim Youth', Working Paper 9, London: Institute for the Study of European Transformations, 2008.

Díaz, Gustavo and Alfonso Merlos, 'The Role of Intelligence in the Battle against Terrorism on the Internet: Revisiting 3/11', Research Paper No. 117, Athens: Research Institute for European and American Studies, 2008.

Disley, E. et al. (2010) Individual disengagement from Al Qa'ida-influenced terrorist groups: A rapid evidence assessment to inform policy and practice in preventing terrorism, London: Home Office

Durodié, Bill and Ng Sue Chia, 'Is Internet Radicalization Possible?' Singapore: S. Rajaratnam School of International Studies, 21 November 2008. As of 18 October 2012: http://www.rsis.edu.sg/publications/Perspective/RSIS1222008.pdf

European Commission's Expert Group on Violent Radicalisation, 'Radicalisation Processes Leading to Acts of Terrorism', 15 May 2008. As of 18 October 2012: www.rikcoolsaet.be/files/art_ip_wz/Expert%20Group%20Report%20Violent%20Radicalisation%20FINAL.pdf

Farrell, Henry, 'The Consequences of the Internet for Politics'. *Annual Review of Political Science,* Vol. 15, 2012, pp.35–52.

Friedland, Jamie and Kenneth Rogerson, *How Political and Social Movements Form on the Internet and How They Change Over Time*, Washington, DC: Institute for Homeland Security Solutions, 2009.

Gartenstein-Ross, Daveed and Laura Grossman, *Homegrown Terrorists in the U.S. and U.K.: An Empirical Examination of the Radicalization Process*, Washington, DC: FDD Press, 2009.

Githens-Mazer, Jonathan, Robert Lambert, Abdul-Haqq Baker, Safiyah Cohen-Baker and Zacharias Pieri, *Muslim Communities' Perspectives on Radicalisation in Leicester, UK*, Aarhus: Centre for Studies of Islamism and Radicalisation, Aarhus University, 2010.

Gray, David H. and Albon Head, 'The Importance of the Internet to the Post-modern Terrorist and its Role as a Form of Safe Haven'. *European Journal of Scientific Research*, Vol. 25, No. 3, 2009, pp.396–404.

Guadagno, Rosanna E., Adam Lankford, Nicole L. Muscanell, Bradley M. Okdie and Debra M. McCallum, 'Social Influence in the Online Recruitment of Terrorists and Terrorist Sympathizers: Implications for Social Psychology Research'. *International Review of Social Psychology*, Vol. 23, No. 1, 2010, pp.25–56.

Horgan, J. and K. Braddock (2010) "Rehabilitating the Terrorists?: Challenges in Assessing the Effectiveness of De-radicalization Programs", Terrorism and Political Violence, 22: 2, 267 – 291

Hunter, Ryan and Daniel Heinke, 'Radicalization of Islamist Terrorists in the Western World'. *FBI Law Enforcement Bulletin*, Vol. 80, No. 9, 2011, pp.25–31.

Hutchinson, William, 'Cyber Influence'. Paper presented at the Australian Information Warfare and Security Conference, Edith Cowan University Research Online, 2009. As of 18 October 2012: http://ro.ecu.edu.au/isw/1/

Kassam, Raheem and Rupert Sutton,'Online Radicalisation: A Case Study'. *Student Rights*, January 2012. As of 18 October 2012: http://www.studentrights.org.uk/userfiles/files/LSBUISocCaseStudy2012(1).pdf

Kenney, Michael, 'Beyond the Internet: Mētis, Techne and the Limitations of Online Artifacts for Islamist Terrorists'. *Terrorism and Political Violence*, Vol. 22, No. 2, 2010, pp.177–197.

Khan, Muqtedar M. A., Reid T. Smith and Onur Tanay, 'Islam, Revolution and Radicalism: The Co-constitution of Reality and Virtuality'. *International Journal of e-Politics*, Vol. 2, No. 3, 2011, pp.1–13.

King, Michael and Donald M. Taylor, 'The Radicalization of Homegrown Jihadists: A Review of Theoretical Models and Social Psychological Evidence'. *Terrorism and Political Violence*, Vol. 23, No. 4, 2011, pp.602–622.

Kirby, Aidan, 'The London Bombers as "Self-starters": A Case Study in Indigenous Radicalization and the Emergence of Autonomous Cliques'. *Studies in Conflict & Terrorism*, Vol. 30, No. 5, 2007, pp.415–428.

Koruth Samuel, Thomas, 'The Lure of Youth into Terrorism'. *Southeast Asia Regional Centre for Counter-Terrorism*, 2011. As of 18 October 2012: http://www.searcct.gov.my/publications/our-publications?id=55

Laqueur, Walter, *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, New York: Oxford University Press, 1999.

Lennings, Christopher J., Krestina L. Amon, Heidi Brummert and Nicholas J. Lennings, 'Grooming for Terror: The Internet and Young People'. *Psychiatry, Psychology and Law*, Vol. 17, No. 3, 2010, pp.424–437.

Lieberman, Joseph and Susan Collins, 'Violent Extremism, the Internet and the Homegrown Terrorist Threat'. Majority & Minority Staff Report, Washington, DC: United States Senate Committee on Homeland Security and Governmental Affairs, 2008.

Mantel, Barbara, 'Terrorism and the Internet: Should Web Sites that Promote Terrorism Be Shut Down?' *CQ Global Researcher*, Vol. 3, No. 11, 2009, pp.129–152.

Ministry of the Interior and Kingdom Relations of the Netherlands, 'Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age'. *Counter-Extremism.org*, 2012. As of 18 October 2012: https://www.counterextremism.org/resources/details/id/110

Mullins, Sam, 'Australian Jihad: Radicalisation and Counter-Terrorism'. *Real Instituto Elcano*, No. 140, 2011a, pp.1–9.

Mullins, Sam, 'Islamist Terrorism and Australia: An Empirical Examination of the 'Home-Grown' Threat'. *Terrorism and Political Violence*, Vol. 23, No. 2, 2011b, pp.254–285.

Musa, Samuel and Samuel Bendett, *Islamic Radicalization in the United States: New Trends and a Proposed Methodology for Disruption*, Washington, DC: Center for Technology and National Security Policy, National Defense University, 2010.

National Coordinator for Counterterrorism, 'Radicalisation in Broader Perspective', 2007. As of 18 October 2012: http://english.nctb.nl/Images/Congresbundel%20UK%20compleet_tcm92-132318.pdf?cp=92&cs=25496

National Coordinator for Counterterrorism, 'Jihadis and the Internet', 2010. As of 18 October 2012: http://www.fas.org/irp/world/netherlands/jihadists.pdf

Nelson, Rick and Ben Bodurian, 'A Growing Terrorist Threat? Assessing "Homegrown" Extremism in the United States', CSIS Homeland Security and Counterterrorism Program Report, Washington, DC: Center for Strategic & International Studies, 2010.

Neumann, Peter R., 'The Internet'. In: *The Adelphi Papers*, Vol. 48, London: Routledge, 2008, pp.53–58.

O'Rourke, Simon, 'Virtual Radicalisation: Challenges for Police'. Edith Cowan University Research Online, 2007. As of 18 October 2012: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1041&context=isw

Patel, Faiza, *Rethinking Radicalization*, New York: Brennan Center for Justice, 2011.

Peters, Ruud, 'The Poldermujahidin: The Radicalization of Young Dutch Muslims'. In: Abicht, Ludo, et al., eds, *Islam and Europe: Challenges and Opportunities*, Leuven: Leuven University Press, 2008, pp.47–61.

Policy Planners' Network, 'Radicalisation: The Role of the Internet', Policy Planners' Network Working Paper, London: Institute for Strategic Dialogue, 2011.

Rabasa, A. et al. (2010) Deradicalizing Islamist extremists, Santa Monica: RAND Corporation.

Reding, A. et al. (2011) SAFIRE inventory of the factors of radicalisation and counterterrorism interventions, Santa Monica: RAND Corporation,

Smiley McDonald, Hope, Nicole Horstmann, Kevin J. Strom and Mark W. Pope, *The Impact of the Internet on Deviant Behavior and Deviant Communities*, Washington, DC: Institute for Homeland Security Solutions, 2009.

Smith, Allison G., 'The Implicit Motives of Terrorist Groups: How the Needs for Affiliation and Power Translate into Death and Destruction'. *Political Psychology*, Vol. 29, No. 1, 2008, pp.55–75.

Speckhard, Anne, ed., 'Psychosocial Organizational and Cultural Aspects of Terrorism: Final Report of the NATO Human Factors and Medicine Research Task Group 140', TR-HFM-140, Durham, NC: Duke University, 2011.

Stenersen, Anne, 'The Internet: A Virtual Training Camp?' *Terrorism and Political Violence*, Vol. 20, No. 2, 2008, pp.215–233.

Sullivan, Robert, 'The Face of Eco-terrorism'. *New York Times*, 20 December 1998. As of 22 October 2012: http://www.nytimes.com/1998/12/20/magazine/the-face-of-eco-terrorism.html?pagewanted=all&src=pm

Thompson, Robin, 'Radicalization and the Use of Social Media'. *Journal of Strategic Security*, Vol. 4, No. 4, 2011, pp.167–190.

Torok, Robyn, 'Facebook Jihad: A Case Study of Recruitment Discourses and Strategies Targeting a Western Female'. In: *Proceedings of the Second International Cyber Resilience Conference*, Perth: Edith Cowan University, 2011a, pp.84–94.

Torok, Robyn, 'The Online Institution: Psychiatric Power as an explanatory model for the normalisation of radicalisation and terrorism'. Paper presented at the IEEE European Intelligence and Security Informatics Conference, Athens, Greece, 12–14 September 2011.

Tucker, David, 'Jihad Dramatically Transformed? Sageman on Jihad and the Internet'. *Homeland Security Affairs*, Vol. 6, No. 1, 2010, pp.1–7.

UK Home Office (2011) 'CONTEST: The United Kingdom's Strategy for Countering Terrorism'. As of 22 October 2012: http://www.homeoffice.gov.uk/publications/counter-terrorism/counter-terrorism-strategy/strategy-contest?view=Binary

UK Home Office and Association of Chief Police Officers, 'Channel: Supporting Individuals Vulnerable to Recruitment by Violent Extremists', 2010. As of 22 October 2012: http://tna.europarchive.org/20100419081706/http:/security.homeoffice.gov.uk/news-publications/publication-search/prevent/channel-guidance?view=Binary

UN Counter-Terrorism Implementation Task Force, 'First Report of the Working Group on Radicalisation and Extremism that Lead to Terrorism: Inventory of State Programmes', 2007. As of 18 October 2012: http://www.un.org/en/terrorism/pdfs/radicalization.pdf

Veldhuis, Tinka and Jørgen Staun, *Islamist Radicalisation: A Root Cause Model*, Clingendael: Netherlands Institute of International Relations, 2009.

Vidino, Lorenzo, 'Radicalization, Linkage, and Diversity'. RAND Corporation, OP-333, 2011. As of 18 October 2012: http://www.rand.org/pubs/occasional_papers/OP333.html

Warner, Benjamin R. and Ryan Neville-Shepard, 'The Polarizing Influence of Fragmented Media: Lessons From Howard Dean'. *Atlantic Journal of Communication*, Vol. 19, No. 4, 2011, pp.201–215.

Wojcieszak, Magdalena, '"Carrying Online Participation Offline": Mobilization by Radical Online Groups and Politically Dissimilar Offline Ties'. *Journal of Communication*, Vol. 59, No. 3, 2009, pp.564–586.

Wojcieszak, Magdalena, 'Computer-mediated False Consensus: Radical Online Groups, Social Networks and News Media'. *Mass Communication and Society*, Vol. 14, No. 4, 2011, pp.527–546.

Yang Hui, Jennifer, 'The Internet in Indonesia: Development and Impact of Radical Websites'. *Studies in Conflict & Terrorism*, Vol. 33, No. 2, 2010, pp.171–191.

Yasin, Nur Azlin Mohamed, 'Social Media and Terrorism in Indonesia: Enhancing or Diluting its Appeal?' S. Rajaratnam School of International Studies, 22 March 2012. As of 18 October 2012: http://www.rsis.edu.sg/publications/Perspective/RSIS0512012.pdf

Zeng, Shuo, Mingfeng Lin and Hsinchun Chen, 'Dynamic User-level Affect Analysis in Social Media: Modeling Violence in the Dark Web'. Paper presented at the IEEE European Intelligence and Security Informatics Conference, Athens, Greece, 12–14 September 2011.

Annex A. Case Studies

A.1. Case Studies A1-A10

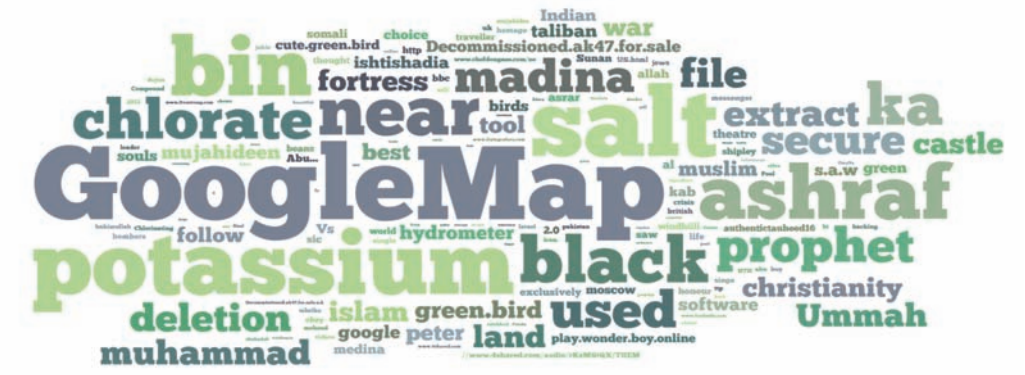
With the exception of A3, a former member of al Qaida who has now disengaged from terrorist activities, the first nine individuals interviewed by the study team are offenders convicted under the Terrorism Act 2000 or the Terrorism Act 2006. We outline their backgrounds below, including details of their ethnic origins, family and other relationships, criminal backgrounds and/or education. Descriptions of the online and offline behaviour of each individual are also included in Tables A.1 – A.8. Obviously some of the information we had access to is pre-selected by the investigating officers, so we cannot give a complete picture of all factors and aspects that relate to their radicalisation.

Table A.1: Case study A1

Background
A1 is a British male who was born in Pakistan and came to the United Kingdom at a young age. During trial proceedings, it was indicated that he lived with his mother. He had a criminal record which included a range of offences such as shoplifting and aggravated assault during the period 1991 to 2011.
Online activity
A1's computer registry activity indicates that he used the internet on a daily basis at home. Figure A1 is a word cloud[23] from A1's computer registry of search terms.

[23] A word cloud indicates through relative size of lettering the relative frequency with which words were searched. The clouds give greater prominence to words that appear more frequently in the source text.

Figure A1: A1's computer registry of search-terms



The above provides a picture of A1's everyday browsing, shopping and information gathering interfused with search terms synonymous with radicalisation. For instance, 'green bird' refers to the foundational Islamist book *In the Hearts of Green Birds* (which relates stories of 'heroic martyrdom'), while there are also attempts to acquire information about where to buy guns – 'decommissioned AK47 for sale'). By early 2011, A1 was accessing bomb-making websites (see the predominance of 'potassium' and 'chlorate' above in A1's search history), downloading beheading videos, and had added Roshanna Choudary[24] to his internet favourites. A1 was also present in peer-to-peer sites. A1 had created five Facebook accounts in total (registered under adopted pseudonyms), each one shut down due to inappropriate content. A1 was security aware in his online behaviour and purchased encryption and file deletion programmes.

Offline activity

While the above description suggests extensive online activity that may be related to radicalising, A1's radicalisation may not have taken place exclusively online. Although there is no evidence to suggest the internet had a catalytic radicalising influence on A1, he stated in court evidence that he attended an Islamic conference in 2010 at which he was given extremist material on a CD. In mid-2011, A1 purchased bomb-making material, including quantities of hydrogen peroxide and other ingredients. A1 also spent time in a number of prisons - an experience which might have served as a possible driver of radicalisation (House of Commons 2012).

[24] Roshanna Choudary is a former student at King's College London accused of the attempted murder of Stephen Timms MP.

Table A.2: Case Study A2

Background

A2 is a British female of Pakistani heritage and is married to A1. The couple first met on the internet. No available evidence suggests that A2 was involved in any form of extremism before meeting A1 (prior to her conviction in 2011 she had no criminal record). The general characterisation of A2's change in behaviour (as relayed in witness reports in court) was a change of direction from an outgoing personality to a more insular and subservient one.

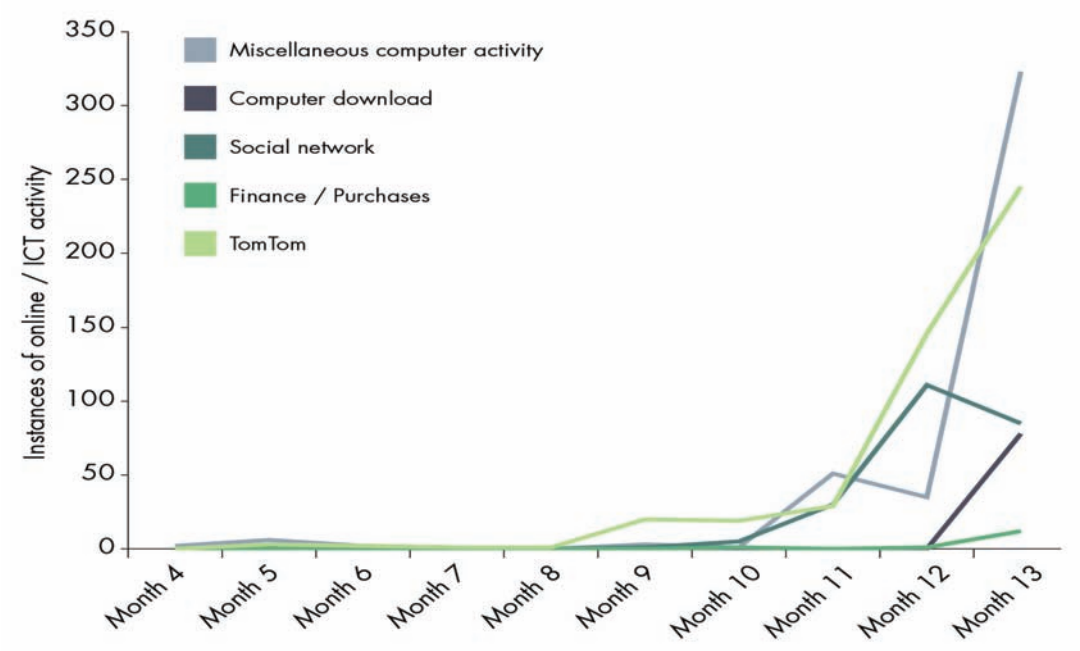
Online activity

Police reports suggest A2's online activity was very much in-step with A1's. A2 also accessed bomb-making websites, downloaded beheading videos (using torrent facilities – see 'btjunkie' listed in A2's search terms in Figure A2 below), and added Roshanna Choudary to her internet favourites (also a prominent search-term below).

Figure A2: A2's computer registry of search-terms

Prominent among A2's search terms were keyword searches for public armed forces events. Police would later find coordinates to a nearby air force base saved in the satellite navigation system she shared with A1. Maintaining security online was also seen as important – settings were set to delete. It's apparent from Figure A3 below that accessing online extremist material became an increasingly prevalent activity for the couple:

Figure A3: Timeline of A1 and A2's online and TomTom (satellite navigation system) activity



Offline activity

Present in other mediums, beyond the internet, was a saturation of extremist media that the couple used (books, television, audio in the car). A1's court evidence suggests that A2 also attended the same Islamic conference at which A1 was given extremist material on CDs).

Table A.3: Case Study A3

Background

A3 grew up in Saudi Arabia and was educated in the Salafistic religious context. In his early life, the internet was absent, and information on 'radical Islam' was passed around circles of friends and acquaintances. In the mid-90s, A3 decided to follow in the footsteps of some friends and travel to Bosnia. Upon witnessing civilian deaths in Bosnia[25], his radicalisation was, he argues, inevitable:

> After everything you've seen, you don't want to go back to

[25] The war between Bosnia and Herzegovina took place between 1992 and 1995 and was a result of the collapse of former Yugoslavia.

> normal life – you feel so detached at that moment from social life, especially if you have a near-death experience. People seem to be having frivolous conversations; they don't have aspirations beyond their own daily life. You start thinking of yourself as elite, a vanguard, and you look for other people like you.

Online activity
A3 spotted the potential to use the internet as a recruitment tool, taking his audience share from "retail to wholesale levels". He identified the spread of the internet, from limited hubs such as internet cafes to every home, as making his job as a recruiter easier. Day to day, A3 was involved in translating violent extremist messages in different languages to English and uploading these onto an extremist website. A3 also identifies the advent of online video as overcoming a limitation that radicalisers had with hard storage devices such as VHS. A3 argued that the internet was important but not transformative for his (and others') radicalisation activities:

> The internet is just another platform. One which allows those that would otherwise be scared of being seen with the wrong people to get engaged, and one which makes the whole process more invisible to the authorities.

Offline activity
A3 judges that he was radicalised prior to the advent of the internet. He is sceptical about how far online activity translates into offline behaviour change. Soon after his time in Bosnia, A3 was identified as a good speaker and became a recruiter and fundraiser. Once he left Saudi Arabia A3 was active for 12 years before he disengaged from terrorist activities.

Table A.4: Case Study A4

Background
A4 converted to Islam on the first anniversary of 7/7 at a prominent Birmingham mosque. Trial documents suggest that A4 was a drug user and was on methadone at the time of his arrest. A4 was described in witness statements by those who knew him as a 'loner'; a comment that reflects his decision to drop out of school for a period of time. Community members noted A4's gradual change of behaviour and adoption of violent extremist views. Acting on community concerns, a police search of A4's flat uncovered explosives and a suicide vest.

Online activity

A4 used the internet from an early age and continued this use through college. The police have established that most of his extremist activity was on the open internet and therefore not encrypted. He did not actively participate in chat rooms but he did search them for answers to questions regarding Islam. The internet gave A4 information on issues ranging from religion and violent extremist propaganda to instructions on how to build suicide vests and explosives (as can be seen from Figure A4 below):

Figure A4: A4's computer registry of search terms.

Offline activity

A4 had a copy of Milestones[26], a book often referenced as a key text in radical Islamist extremism at his address, but police suggest that the internet was his extremist library. Originally, A4 claimed that his decision to search for answers online was a result of being unsuccessful in finding a suitable mentor in the mosques he searched. A4 has been described as having a compulsive personality and had a previous criminal conviction. Trial documents suggest that in the months leading up to his arrest, he had a number of friends with whom he shared information about what he was doing and thinking. He was arrested after a tip-off from the local community.

Table A.5: Case Study A5

Background

A5 is a white British male from the North of England. Following the separation of his

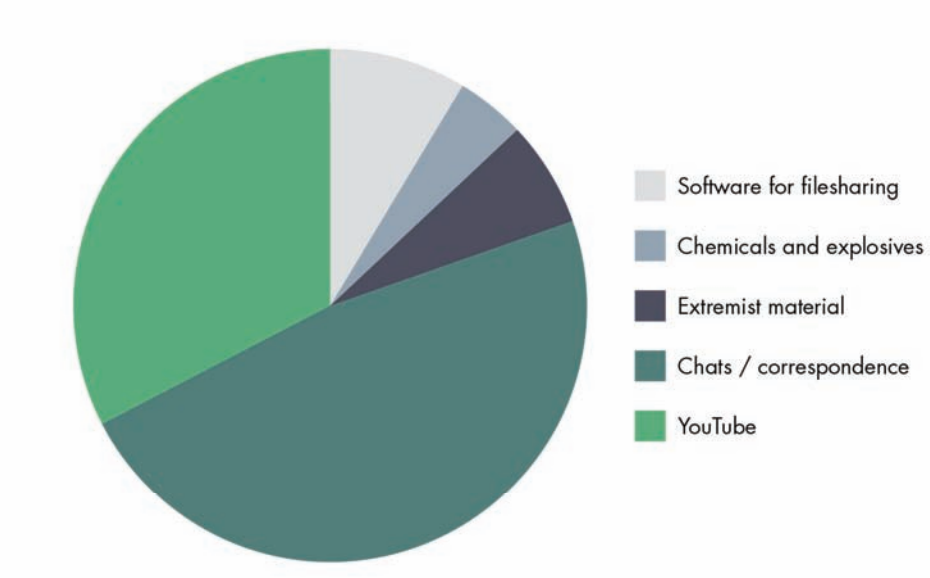
[26] Milestones is a book by Sayyid Qutb in which he makes a call to re-create the Muslim world strictly based on the Qu'ran. The book, the author and his thinking had influence on Islamic terror groups and extremists.

parents, A5 moved in with his father. In one of his interviews, A5 noted the strong influence of the racist views held by his father. At that point, his father was a member of an online right-wing group. A5 became involved in the group without his father's involvement or knowledge. Following the arrest of his father for terrorism offences, A5 was also arrested and charged with a number of offences that included inciting racial violence.

Online activity

A5 observed that he had used the internet for "*as long as I can remember*". He began to engage in online debates (the largest portion of his time spent online as we can see in Figure A5 below), contacting group members of the online right-wing group via Skype and MSN Messenger and developing friendships with white supremacists from across Europe. We can also see below that A5 searched for extremist material and chemicals/explosives.

Figure A5: Breakdown of A5's online activity



According to A5, his online activities made him feel part of a group and important. He became a committee member and was approached numerous times to help other members (such as helping to create images and leaflets). A5's online right-wing group activity lasted for one and a half years. He claims that, following this period, endless debate online grew quite tiresome.

Offline activity

As noted above, A5's father is a prominent figure in his life. Interview evidence indicates that A5's father regularly reprimanded him for listening to rap music and watching television programmes which featured ethnic minorities in prominent roles. Moreover, according to his testimony his father threatened to "*hang him if he was found sleeping with [a] black woman*". A5 became curious about his father's interests and started to search his

father's extreme right-wing websites. A5 suggested that his personal relationship with his father offline was a factor in his radicalisation and online behaviour; A5 acknowledged that he developed a more 'friendly relationship' with his father when he told him about his online activities. A5 was mindful not to discuss his online behaviour more widely, however, fearing the stigma. Other than spending time online, A5 would receive some books (like the Protocols of the Elders of Zion[27]) from his father.

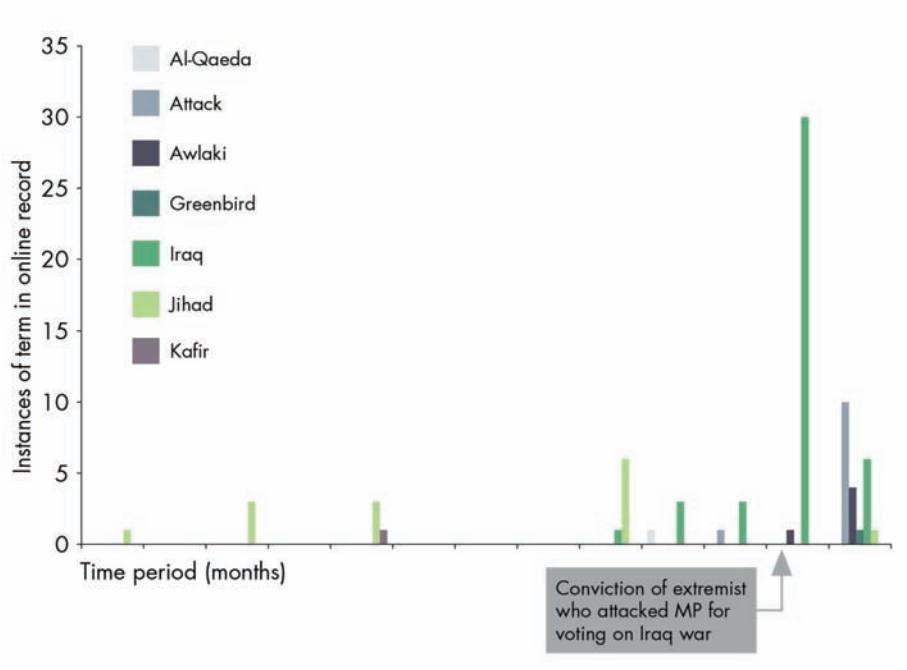
Table A.6: Case Study A6

Background
A6 is a British Asian who, according to police and social services reports, is considered as coming from an unstable family. At the age of 15, A6 moved into an area of London that was intensively targeted by recruiters of the now-proscribed group al-Muhajiroun[28]. A6 socialised with a group of friends in al-Muhajiroun and trial evidence suggested that he was influenced by them in his pathway to radicalisation.
Online activity
A6 used the internet to discuss religious issues and police reports suggest that he set out to teach and influence others. This activity was mainly undertaken through postings and blogs, and he also gained administrative rights to a prominent Islamic forum. Below, we can see a representation of A6's online activity and keyword searches. The spike in activity comes directly after the conviction of Roshanna Choudary.

[27] The Protocols of Zion is an anti-Semitic hoax purporting to describe a Jewish plan for global domination.

[28] Al-Muhajiroun is a banned Salafi-Wahabi Islamist terrorist organisation that was based in Britain. Michael Adebolajo, the man accused of killing Lee Rigby in a terrorist attack in Woolwich, attended al-Muhajiroun meetings and demonstrations.

Figure A6: A6's use of keywords in online activity synthesised with offline timeline



Recovered posts on Islamic sites suggest A6 would not accept moderate discussions quoting the Qur'an to counter violent messages. A6's postings suggest that he considered it a Muslim's duty to undertake jihad. A6 was engaged in this extremist online activity at the time of the trial of Roshana Choudhry. Angry that Choudhry was convicted of her offence, A6 posted messages on the internet, claiming that she was a heroine and that other people should follow in her footsteps. He encouraged his readers to '*pick up the sword of jihad*', and provided them with information on how to find their local Member of Parliament. He also created links to knives for sale on Tesco's website.

Offline activity

A6's affiliation with al- Muhajiroun began with a physical introduction to a member during a march in front of the US embassy. A6 would travel to Dorset every weekend to take part in da'waa stalls. A lot of his spare time was channelled towards preparing for his time on the stalls (i.e. designing leaflets). Spurred by his online debating experience, A6 was also working hard at building up his skills to speak offline (he would practice by making homemade videos).

Table A.7: Case Studies A7, A8 and A9

Background
A7 is a British Asian of Indian heritage. Trial evidence and police accounts suggest that A7 is a young Muslim from a very socially conservative family resident in a town in which ethnic communities are known to self-segregate. After attending a state primary school, his family enrolled him in an Islamic school. By the age of 15 he had attained the status of *hafiz,* a title awarded to those who know the Qur'an by heart. In his early teens A7 struck up a close friendship with two individuals, A8 and A9 (also discussed below). A8 and A9 are British Asian brothers of Indian heritage. Trial evidence suggested that their parents, who lived next door, were largely unaware of their sons' extremist activities.
Online activity
A7, A8 and A9 created a 'resistance group' with an online profile, claiming an al Qa'ida sponsored remit and threatening national political figures. They made numerous videos using social media software, including images of them practising ambushes and playing with a self-loading pistol and two machetes. When A8 and A9's house was searched, police found 'an arsenal' of weaponry and military equipment including crossbows, knives and machetes. Live ammunition also was recovered at the address. All three downloaded a vast quantity of extremist material onto A7's laptop, various USB sticks and mobile phones. A7 published material on the internet which was designed not only to persuade people to commit murder in the UK, but also to spread the idea that al Qa'ida had established an organisation in the UK and to invite support for it. For more than a year A7 regularly posted messages on two websites and distributed material by posting links to information on topics such as bomb-making. He used multiple identities that he would regularly play off each other in order to build his status online.
Offline related activity
A8 and A9 developed an interest in survival training and equipment which may have been influenced by material they identified online. A8 and A9 were regular visitors to outdoor pursuits shops in their town as well as the local hunting/fishing shops where they procured some tools that could be used as weapons. Offline, the 'resistance group' practised military manoeuvres in the local park and surrounding countryside. When the police arrived at the home of A7 they found gasoline, Hezbollah bomb-building manuals, a suicide bomb belt, a missile, explosives and detonators inside.

Table A.8: Case Study A10

Background
A10 is a British male of South Asian origin. His family lives in the north of England and police accounts suggest they were well-respected among the local community. A significant change in A10's offline attitudes and behaviour led his school to raise concerns.
Online activity
At a young age, A10 began to do his own online research into the conflicts in Afghanistan and Pakistan and western foreign policy. Through the internet, he was identified and approached by a terrorist facilitator in Pakistan who made regular visits to the UK. Trial documents suggest that the facilitator discussed a range of issues with A10 - including how someone might smuggle a sword through airport security - feeding and shaping his interests. Interview evidence suggests that by this point A10 began to discuss arrangements for military training in Pakistan. A10 had collected a large quantity of material from the internet by the time of his arrest, including extremist material, information on chemical weapons and instructions on how to make napalm.
Offline activity
It was his introduction to a terrorist facilitator at the central mosque in Dewsbury that inspired A10 to search online for information on bomb-making and extremist material. Following his introduction at the mosque, the facilitator and A10 began to communicate regularly online. Evidence suggests that A10 was being groomed for a mission in the UK.

A.2. Case Studies B1-B5

With the exception of A3, the individuals listed above were all convicted of terrorism offences. In order to understand the challenge facing the police and multi-agency partners, this study also reviewed a small sample of people deemed by the police to be at risk of radicalisation. These individuals were referred to the police by local government organisations and considered to be within the remit of the *Prevent* intervention programme, Channel. Due to the potentially on-going nature of the intervention strategies around these individuals the information we can convey is limited, high-level, and focused on providing illustrations of the role of the internet in radicalisation.

Table A.9: Case Studies B1-B5

B1
B1 is a 15 year old male student based in the UK. Concerns about B1 were raised by one of his secondary school teachers. B1 had told the teacher that he had been looking at al Qa'ida online and supported their agenda. He also expressed a desire to travel abroad to an al Qa'ida training camp. The incident was referred to community policing (Channel) who made the subsequent discovery that B1 was being influenced by an older figure online (based in the US). Identifying that B1 was potentially being radicalised over the internet, Channel assisted the school in making a referral to Child Services. At the same time, in cooperation with the school and police, Channel arranged for B1's computer to be seized and examined in order to identify the purported radicaliser(s).
B2
B2 is a middle aged white British male and a member of the English Defence League (EDL)[29]. B2 joined the EDL shortly after seeing its members demonstrating in towns and cities across the UK. In his own words, his determination to join stems from witnessing an influx of "holier than thou" persons of Muslim faith into his neighbourhood, who he alleges were involved in illegal behaviour (i.e. drug-dealing). B2's online activity mostly gravitated around engaging with fellow EDL members and organising future demonstrations. B2 enjoyed trading insults with members of an opposition website – the Muslim Defence League (MDL). For the future, B2 is committed to the EDL: I've been to all of the demos so far and will keep going to them because I believe in what we are doing. Somebody has got to stand up and I don't see anyone else doing anything.

[29] The EDL is a far-right street protest movement. The group opposes what it considers to be a spread of Islamism, Sharia law and Islamic extremism in the UK.

B3

B3 is a middle aged Asian female who has been diagnosed with a mental illness. She is a regular user of the internet and particularly Facebook. B3 has extreme views (admitting that some of her thoughts are not for moderates) and while she does not believe in violence, she becomes more vocal about her political views and beliefs when on her medication. Recently B3 threatened a female and was detained in hospital due to her deteriorating condition.

B4

B4 is a white male, aged 16 with autism and behavioural issues. His mother had expressed concerns about her son becoming an animal rights activist. When police officers visited the home of B4, it became apparent from speaking to the family that B4 spent most of his time in his bedroom unsupervised on the internet, and had posted several videos criticising people who eat meat. However, a review of material on his computer found no extreme content.

B5

B5 is a white male and has been described as a loner who spent most of his time on the internet. B5 sent an email to his school head teacher threatening to kill him and other teachers unless he received a £30,000 ransom. According to B5, there were a number of explosives planted around the school building. When questioned by police, B5 admitted to having looked at explosives on the internet.