IDENTIFYING FOREIGN TERRORIST FIGHTERS

The Role of Public-Private Partnership, Information Sharing and Financial Intelligence

Tom Keatinge

ICCT International Centre for Counter-Terrorism - The Hague

RUSI www.rusi.org

About ICCT – The Hague

The International Centre for Counter-Terrorism – The Hague (ICCT) is an independent knowledge centre that focuses on information creation, collation and dissemination pertaining to the preventative and international legal aspects of counter-terrorism. The core of ICCT's work centres on such themes as de- and counter-radicalisation, human rights, impunity, the rule of law and communication in relation to counter-terrorism. Functioning as a nucleus within the international counter-terrorism network, ICCT – The Hague endeavours to connect academics, policy-makers and practitioners by providing a platform for productive collaboration, practical research, exchange of expertise and analysis of relevant scholarly findings. By connecting the knowledge of experts to the issues that policy-makers are confronted with, ICCT – The Hague contributes to the strengthening of both research and policy. Consequently, avenues to new and innovative solutions are identified, which will reinforce both human rights and security.

Contact:
ICCT – The Hague Koningin Julianaplein 10 P.O. Box 13228 2501 EE, The Hague, The Netherlands

T: +31 (0)70 800 9531 E: info@icct.nl

All papers can be downloaded free of charge at www.icct.nl Stay up to date with ICCT, follow us online on Facebook, Twitter and LinkedIn.

About RUSI

The Royal United Services Institute (RUSI) is an independent think tank engaged in cutting edge defence and security research. A unique institution, founded in 1831 by the Duke of Wellington, RUSI embodies nearly two centuries of forward thinking, free discussion and careful reflection on defence and security matters.

www.rusi.org

About RUSI's Centre for Financial Crime and Security Studies

RUSI's new Centre for Financial Crime and Security Studies (CFCS) brings much-needed research and analytical capacity to support the work of the private sector, the UK government, and international governmental and multilateral partners in addressing the challenges posed by financial crime and illicit finance in all its forms. The programme focuses on both policy matters related to national and international efforts to tackle illicit finance as well as topical issues related to threat finance such as terrorist financing, the use of financial intelligence, and counter-proliferation finance. The team includes expertise from banking, academia and law-enforcement agencies.

Identifying Foreign Terrorist Fighters

The Role of Public-Private Partnership, Information Sharing and Financial Intelligence

Tom Keatinge

www.icct.nl

www.rusi.org

The views expressed in this paper are the author's own, and do not necessarily reflect those of RUSI or any other institutions with which the author is associated.

Comments pertaining to this report are invited and should be forwarded to:
Tom Keatinge, Director, Centre for Financial Crime and Security Studies, Royal United Services Institute, Whitehall, London, SW1A 2ET, United Kingdom, or via email to tomk@rusi.org

www.rusi.org/publications

Printed in the UK by Stephen Austin and Sons, Ltd.

Contents

Acknowledgements

This paper has benefited from the support of a number of organisations and individuals whom I would like to thank. The International Centre for Counter-Terrorism – The Hague (ICCT) has kindly sponsored and supported this work, during which time I have been ably supported by B W Morgan who gathered valuable primary research. This support has been supplemented by Charlie Edwards and the team at the Royal United Services Institute (RUSI) since I joined the Institute in December 2014. In particular I would like to acknowledge the contribution of Chris Edwards who provided me with valuable research support and impetus. I would also like to thank the Airey Neave Trust for its kind contribution towards the publication costs of this paper.

Finally, I would particularly like to thank Shiraz Maher at the International Centre for the Study of Radicalisation and Political Violence (ICSR) who generously provided access to the Centre's database of online, social-media material from which all screenshots reproduced in this paper are taken.

Acronyms and Abbreviations

AML/CTF	Anti-money laundering and countering the financing of terrorism
AUSTRAC	Australian Transaction Reports and Analysis Centre
ATM	Automated teller machine, or cashpoint
FFIEC	Federal Financial Institutions Examination Council
FATF	Financial Action Task Force
FININT	Financial intelligence
FIU	Financial intelligence unit
FTF	Foreign terrorist fighter
ICSR	International Centre for the Study of Radicalisation and Political Violence, King's College London
ISI	Islamic State of Iraq
ISIS	Islamic State of Iraq and Syria, also known as Daesh
JMLIT	Joint Money Laundering Intelligence Taskforce
JMLSG	Joint Money Laundering Steering Group
NCA	National Crime Agency
NTFIU	National Terrorist Financial Investigation Unit
OECD	Organisation for Economic Co-operation and Development
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SAR	Suspicious activity report
TFTP	Terrorist Finance Tracking Program

Executive Summary

Since 9/11, financial institutions have found themselves placed squarely on the front line of efforts to combat terrorism: countering terrorist financing has been a core element of the global counter-terrorism architecture since President George W Bush signed Executive Order 13224 promising to starve terrorists of funding.[1] Financial institutions have played valuable 'post-event' forensic roles, but despite the apparently immense troves of data they hold, their effective involvement in the identification and disruption of terrorist intentions or activity remains elusive. With global authorities consumed with the mushrooming growth of 'foreign terrorist fighters' (FTFs),[2] it seems timely to revisit the question of how financial institutions can play a more preventative role in countering terrorist threats. As the intergovernmental Financial Action Task Force (FATF) noted recently, 'greater domestic cooperation among AML/CFT [anti-money laundering and countering the financing of terrorism] bodies and other authorities'[3] is needed to tackle funding of FTFs.[4] Banks must play a key role in the development of this architecture.

The issue of FTFs flowing to and from the conflict in Syria is likely to shape the international security agenda for the foreseeable future. According to Thomas Hegghammer, 'at this rate, the foreign fighter flow into Syria looks set to extend the life of the jihadi movement by a generation'.[5] An October 2014 Briefing Paper from the Royal United Services Institute (RUSI) assessed that 'it is this community of foreign fighters that poses an immediate terrorist threat to the West',[6] with one of the paper's key judgments being that 'British

1. US Department of the Treasury, 'Contributions by the Department of the Treasury to the Financial War on Terrorism', fact sheet, September 2002, p. 2, <http://www.treasury.gov/press-center/press-releases/Documents/2002910184556291211.pdf>, accessed 11 June 2015.
2. Consistent with UN Security Council Resolution 2178, this paper uses the acronym FTF to refer to those foreign terrorist fighters 'who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training'.
3. AML/CFT refers to anti-money laundering and countering the financing of terrorism, the two primary activities that the FATF addresses with the standards it publishes. The so-called 40 Recommendations provide guidelines for countries and financial institutions with regards to ways in which money laundering and terrorist financing can be disrupted.
4. FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)', February 2015, p. 36, <http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf>, accessed 11 June 2015.
5. Thomas Hegghammer, 'Syria's Foreign Fighters', ForeignPolicy.com, 9 December 2013, <http://foreignpolicy.com/2013/12/09/syrias-foreign-fighters/>, accessed 11 June 2015.
6. Raffaello Pantucci and Clare Ellis, 'The Threat of ISIS to the UK: RUSI Threat Assessment', RUSI Briefing Paper, October 2014, p. 1.

citizens who have joined terrorist groups in Syria and Iraq pose a threat to the UK.'[7] The UK is certainly not alone in Europe in facing this threat.[8] Evidence suggests these fears are now being realised. Not only does Daesh (also known as the Islamic State of Iraq and Syria, ISIS) urge its supporters, through its magazine *Dabiq*, to target 'citizens of crusader nations … wherever they can be found';[9] but such attacks are already taking place, perpetrated by the likes of FTF returnee Mehdi Nemmouche, who is alleged to have killed four people in the Jewish Museum in Brussels in May 2014.[10]

The issue of foreign fighters is not new. Jihadi conflicts over the past thirty years in Afghanistan, Bosnia and Somalia have attracted fighters from across the globe. Further back, the Spanish Civil War (1936–39) was a magnet for those committed to fighting fascism. And indeed as far back as the 1590s returning foreign fighters were a concern for England as individuals such as Guy Fawkes returned from fighting with the Spanish in the Eighty Years' War (1568–1648).[11] However, both the scale of the issue in the context of the Syrian conflict and the speed with which the numbers have risen have caught international security authorities off guard, which – it would seem – have only belatedly appreciated the magnitude of the challenge.

Whilst there has been much discussion and debate about who these travelling fighters are, their motivations, and the threats they pose, the majority of this analysis has focused on the role of social media in this phenomenon. This Occasional Paper, by contrast, considers another source of data that could inform this analysis, namely the financial intelligence (FININT) generated by the huge quantities of transaction data gathered by the financial-services industry as it processes bank transfers, ATM withdrawals and credit-card transactions. It asks what barriers exist to greater partnership and information sharing between the security authorities and the financial-services industry in tackling terrorism. And whether, within the parameters of acceptable data-privacy restrictions, an intelligent and intelligence-led relationship between the security authorities and the financial-services industry could provide greater and more timely insight into which individuals are travelling to Syria or are already in-country, and (perhaps most importantly) who,

7. *Ibid.*, p. 3.
8. See for example, Piotr Bakowski and Laura Puccio, '"Foreign Fighters": Member States' Responses and EU Action in an International Context', European Parliament Briefing, February 2015, <http://www.europarl.europa.eu/EPRS/EPRS-Briefing-548980-Foreign-fighters-FINAL.pdf>, accessed 11 June 2015.
9. *Dabiq*, 'The Failed Crusade' (No. 4, July 2014), p. 44.
10. *BBC News*, 'Brussels Jewish Museum Murders: Nemmouche to Be Extradited', 26 June 2014.
11. House of Commons Home Affairs Committee, 'Counter-Terrorism', Seventeenth Report of Session 2013–14, HC 231, 9 May 2014, p. 13, <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf>, accessed 12 June 2015.

having been exposed to the extremist ideology espoused by groups such Daesh, has returned home.

In 2004, the 9/11 Commission's 'Monograph on Terrorist Financing' cast doubt on the extent to which arming bank personnel with intelligence would give them a better idea of what they are looking for and allow them 'to ferret out the terrorists among their customers'.[12] This paper reassesses that assertion and concludes that, over a decade later, the lack of partnership and information sharing between the public and private sectors is dramatically hindering the valuable role banks could play in assisting in disrupting terrorism. Advances in technology and transaction-monitoring systems have immeasurably improved the capabilities of banks and other financial institutions, such as large-scale remittance companies, to play the front-line role that is required of them by the authorities. As the 'Monograph on Terrorist Financing' acknowledged, 'Although financial institutions lack information that can enable them to identify terrorists, they have information that can be absolutely vital in finding terrorists'.[13] This statement has only become more relevant since 2004. Banks must be empowered to do the job that the authorities have delegated to them. Tentative steps have been taken in this regard, such as the founding of the UK Financial Sector Forum and Joint Money Laundering Intelligence Taskforce (JMLIT) – these are welcome, but finance and terrorism are global operations and without effective cross-border public-private-sector partnership and information sharing, banks will continue to hunt blindly. Unlike money laundering, terrorist financing is highly dynamic and subject to geopolitical developments. As Richard Barrett, the former co-ordinator of the UN Al-Qa'ida and Taliban Monitoring Team, has underlined, 'States cannot expect the private sector to have a better idea of what terrorist financing looks like than the states themselves'.[14]

The security threat posed by FTFs – and the apparent struggle faced by national security authorities in identifying and tracking such individuals – provides an ideal and timely platform from which to discuss the role that banks can play in countering terrorist threats, which requires urgent re-evaluation and enhancement. As the FATF has observed, 'the effectiveness of authorities at both detecting and investigating terrorist activity is significantly enhanced when counter-terrorist intelligence and financial information are used together'.[15]

12. John Roth, Douglas Greenburg and Serena Wille, 'Monograph on Terrorist Financing', staff report to the National Commission on Terrorist Attacks upon the United States, 2004, p. 63, <http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf>, accessed 17 June 2015.
13. *Ibid.*, p. 58.
14. Richard Barrett, 'Preventing the Financing of Terrorism', *Case Western Reserve Journal of International Law* (Vol. 44, No. 3, 2011), p. 730.
15. FATF, 'Terrorist Financing', 2008, p. 4, <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf>, accessed 12 June 2015.

With this in mind, this paper offers four observations and recommendations that should be urgently addressed if national authorities are to make effective use of what remains a neglected but potentially valuable counter-terrorism tool.

First, the authorities must properly understand what types of information and intelligence are of value to the banking community in identifying terrorist activity. The sharing of classified information is clearly problematic. Even if individuals in banks are cleared to receive such intelligence, the use and further sharing of this information is challenging within a bank. However, bankers, in general, do not want or need classified information. They require thematic rather than entity-level information that allows them to deploy algorithms and filters within their transaction monitoring that alerts them to cases that call for further investigation. It is a clichéd image, but the more that the authorities can reduce the size of the haystack of information through which banks are required to sift, the more likely banks are to provide high-quality information in return.

Secondly, national security and law-enforcement agencies need to develop processes for sharing specific threat data with banks. Establishing a co-ordinated and intelligent process of producing and disseminating timely and detailed guidance to banks is a critical link that has been absent for too long – although some nascent steps are finally being taken. For example, in the UK, the JMLIT has been established which can be used by the authorities to alert bank members of the taskforce to details disclosed to them via suspicious activity reports. The British Bankers' Association will also soon launch its Financial Crime Alerts Service that aims to use real-time intelligence pooled from twelve partner agencies – including the National Crime Agency – to help banks tackle financial crime.[16] By disseminating intelligence in this manner, the authorities can ensure that relevant security information is shared across the banking community as well as between individual banks and the authorities, thus ensuring information vacuums are avoided.

Thirdly, and closely related, barriers to information sharing within the public sector and within individual banks must be addressed. Systems such as Ma^{3}tch being developed by FIU.net could play a valuable role in facilitating the matching of cross-border FININT, whilst an urgent overhaul of the information-sharing regulatory framework for banks also needs to be undertaken. As things stand, on both counts, the restriction on information sharing significantly hampers efforts to tackle money laundering and terrorist financing.

16. British Bankers' Association, 'Banks Team up with Government to Combat Cyber Criminals and Fraudsters', 23 September 2014, <https://www.bba.org.uk/news/press-releases/banks-team-up-with-government-to-combat-cyber-criminals-and-fraudsters/#.VRgs347F-Sp>, accessed 12 June 2015.

Finally, the authorities need to work to produce forward-looking financial threat assessments. Too much guidance is provided on a historical basis. For example, recent reports from the FATF and other multilateral organisations such as the UN provide some useful insights into the past modus operandi of Daesh, but give no consideration to how this model might evolve. Financial institutions require this insight if they are to be able to contribute the valuable intelligence they may hold. Whereas financial institutions have a significant pool of experience on which to draw when tackling fraud and other forms of financial crime, they are less well equipped to identify activity regarding FTFs unless supplied with typologies by those better informed, namely the security authorities.

Conclusion

The FTF phenomenon has caught security authorities across the globe off guard. Authorities in many Western capitals only awoke, belatedly, to the threat once many hundreds of their citizens had made the journey to Syria and had begun openly to promote their actions via social media. Significant resources are now being mobilised to combat the threat posed by returning radicalised jihadi fighters. For too long, banks have been held accountable for protecting the financial borders without being appropriately empowered to do so effectively. The threat posed by FTFs should provide urgent impetus for this weakness to be addressed, using the financial footprints left by FTFs to illuminate both their activity and that of the wider network to which they are connected. The financial sector has the capability to act as a significant 'force multiplier' for the security authorities.[17] Neglecting this capability is a security weakness that must be urgently addressed.

17. David Cohen, US under secretary for terrorism and financial intelligence, speaking at the Royal United Services Institute (RUSI), June 2014, London.

Introduction

A brief scan of media reports and academic research confirms that in the view of many, today's most pressing global security threat is the risk created by individuals travelling to fight with groups in Syria and Iraq where they may be radicalised and may then return home with the intent of inflicting violence on those they view as enemies of Islam. These so-called 'foreign fighters' have flocked to Syria and Iraq in their thousands, although estimates vary. Recent testimony by a senior US counter-terrorism official suggested that more than 20,000 fighters from more than ninety countries have travelled to Syria,[1] with the vast majority coming from Arab states. However, a significant minority – some suggest as many as 4,000 – come from Western states, including most countries of the EU, the US, Australia, Canada and New Zealand. Russia is also well represented.[2] As the Soufan Group has observed:[3]

> There is considerable international concern at what these young men – and some women – will do once they leave Syria, and although almost all appear … to go without a thought of what next, the experience of being in a war zone and exposed to the radicalizing influences of sectarianism and other forms of extremism are bound to have an impact on their ability and willingness to resume their former lives.

Whilst the authorities are now well aware of the 'foreign terrorist fighter' (FTF) phenomenon, the role the Syrian conflict has played in attracting young men to travel to the region to fight, and the risk they may pose if they return home, awareness of this issue seemed to dawn slowly. For example, the UK Parliament's Home Affairs Committee launched an enquiry into counter-terrorism in July 2013, two years after the start of the conflict in Syria, with no mention of the risk to the UK of FTFs. By the time its report was published in May 2014, FTFs featured as a central and key threat, with the report noting that the risk had 'only recently begun to be perceived as a major threat to the UK', something to which the Home Office's submission to the committee in October 2013 had not even referred.[4]

---

1. Mark Hosenball, 'Foreign Fighters Still Flowing to Syria, U.S. Intelligence Says', *Reuters*, 10 February 2015.
2. Peter R Neumann, 'Foreign Fighter Total in Syria/Iraq Now Exceeds 20,000; Surpasses Afghanistan Conflict in the 1980s', ICSR, 26 January 2015, <http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/>, accessed 12 June 2015.
3. Richard Barrett, 'Foreign Fighters in Syria', Soufan Group, June 2014, p. 9, <http://soufangroup.com/wp-content/uploads/2014/06/TSG-Foreign-Fighters-in-Syria.pdf>, accessed 12 June 2015.
4. House of Commons Home Affairs Committee, 'Counter-Terrorism', Seventeenth Report of Session 2013–14, HC 231, 9 May 2014, p. 20, <http://www.

As can be seen from the evidence received by the Home Affairs Committee, a major contributor to the illumination of the issue of Western citizens travelling to Syria to fight with, in the main, extremist groups was the social-media analysis undertaken by academic organisations such as the International Centre for the Study of Radicalisation and Political Violence (ICSR) at King's College London. Many of the individuals travelling to Syria to fight appeared to allow their desire to communicate with friends back home and their wish to publicise their adventures to trump any form of operational security. As one analyst has noted, 'This is the most socially mediated conflict in history … they want to use it [social media] in order to inspire people to come out and join their cause'.[5] Identifying and tracking their activities online is in many cases straightforward.

The role that social-media analysis can play in identifying and tracking FTFs has been well reviewed.[6] However, there is another form of 'footprint' that has been substantially overlooked in the attempts to identify and track those individuals travelling to fight in Syria and Iraq, namely the financial intelligence (FININT) that can be garnered from the transaction data gathered by banks and credit-card companies as they routinely monitor use for fraudulent or criminal activity.

FININT has proven to be a highly effective tool when used in the forensic examination of terrorist events once they have occurred, and has, on a few occasions, assisted in unearthing or monitoring terrorist plans.[7] This Occasional Paper examines specifically whether FININT can play an important role in the *early* identification of those individuals either planning to travel or having already travelled to Syria (or other jihadi theatres). Can an informed

publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf>, accessed 12 June 2015.

5. *BBC News*, 'Syria: Report Shows How Foreign Fighters Use Social Media', 15 April 2014.
6. See Joseph A Carter, Shiraz Maher and Peter R Neumann, 'Who Inspires the Syrian Foreign Fighters?', ICSR, 15 April 2014, <http://icsr.info/2014/04/icsr-insight-inspires-syrian-foreign-fighters/>, accessed 17 June 2015; UN Security Council, 'Security Council Unanimously Adopts Resolution Condemning Violent Extremism, Underscoring Need to Prevent Travel, Support for Foreign Terrorist Fighters', meetings coverage, SC11580, 24 September 2014; Jytte Klausen, 'Tweeting the *Jihad*: Social Media Networks of Western Foreign Fighters in Syria and Iraq', *Studies in Conflict and Terrorism* (Vol. 38, No. 1, 2015).
7. For example, according to the US Treasury Department, 'Since its inception in 2001, the [Terrorist Finance Tracking Programme] has provided valuable lead information that has aided in the prevention of many terrorist attacks and in the investigation of many of the most visible and violent terrorist attacks and attempted attacks'. US Treasury Department, 'Terrorist Finance Tracking Program: Questions and Answers', <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/tftp_brochure_05062014.pdf>, accessed 12 June 2015.

and guided financial-services industry provide valuable intelligence to the authorities?

Three primary factors suggest that this could indeed be the case:[8]

- Those that travel to Syria to fight are generally young and use ATMs, debit and credit cards naturally and freely, thereby leaving a significant financial footprint
- Turkey is the main transit hub for Westerners travelling to join the conflict, particularly the extremist groups that are primarily located close to the Syrian–Turkish border. Turkey benefits from a relatively advanced banking system with the widespread availability of ATMs, and credit- and debit-card payment terminals. There are thus many opportunities for those travelling from Western countries to northern Syria to leave a financial footprint
- Those travelling to this region to join the fight seem relatively unconcerned about masking their movements, as can be seen from the way in which they use Twitter, Facebook and other social media to advertise their activities. It therefore seems probable that they will be less than careful in the way in which they use financial services whilst preparing for their trip (such as buying airline tickets) and during the journey to the border region.

Box 1: What is FININT?

The collection of FININT involves gathering information about the financial activities of an organisation or individual in order to gain a better understanding of the actor's capabilities and plans. The nature of modern-day financial transactions and the due diligence that banks and other regulated institutions that handle or facilitate the movement of money are required to undertake means that individuals and organisations are highly likely to leave regular and revealing electronic financial footprints. For example, the use of ATMs or credit-card terminals can provide valuable geolocation information and regular financial transactions reveal insights into the habits of account holders. Short of dealing entirely in cash and outside any formal financial channels, covering a financial trail is extremely challenging.

FININT has a further benefit, often revealed as being fundamental to the investigation or disruption of criminal or terrorist activity. FININT can reveal

8. These conclusions are informed via the range of interviews with banks, money-service companies and other individuals who have studied relevant transaction data.

the activities of not just a person or organisation of interest, but also the network with which they interact and operate. Financial transactions connect people and groups across the globe and can provide revealing details of accomplices, facilitators and partners.

Governments have multiple ways of exploiting FININT. First, countries are required by Recommendation 29 of the Financial Action Task Force (FATF)[1] to:[2]

> [E]stablish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis.

In general, the financial intelligence unit (FIU) acts as the cornerstone of a country's defence against illicit finance but it relies on receiving information from banks and other institutions that are required by most national laws (as directed by the FATF) to file suspicious activity reports (SARs). Secondly, FININT is also generated by investigations being undertaken by law-enforcement and security authorities. In the UK, responsibility for conducting investigations into such financial leads is conducted by the National Terrorist Financial Investigation Unit (NTFIU), a body housed within London's Metropolitan Police. Finally, a state's security services may use FININT as part of their work to 'seek to obtain detailed knowledge of target organisations, their key personalities, infrastructure, intentions, plans, and capabilities'.[3]

Outside government, financial institutions are increasingly establishing their own, in-house FIUs in order to ensure they understand the nature of the money flows they are facilitating and to co-ordinate their communication (primarily via the filing of SARs) with national FIUs. Such in-house FIUs often include investigation units that keep track of and assess open-source information that can help a financial institution be more effective in contributing to the effort to tackle financial crime in all its forms.

---

1. The FATF, based at the Organisation for Economic Co-operation and Development (OECD) in Paris, is the global standard-setter for international efforts to tackle money laundering and terrorist financing. FATF publishes 40 Recommendations against which national AML/CTF (anti-money laundering and countering the financing of terrorism) efforts are regularly assessed.
2. FATF, 'The FATF Recommendations', February 2012, p. 24, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf>, accessed 12 June 2015.
3. MI5, 'Gathering Intelligence', <https://www.mi5.gov.uk/home/about-us/how-we-operate/gathering-intelligence.html>, accessed 12 June 2015.

Underpinning all these initiatives is the belief that information gathered from the financial transactions made by individuals or organisations can contribute valuable insight into the operations of bad actors and help identify the networks in and with which they operate, a capability that could prove invaluable in the identification of FTFs.[4]

4. For example, at the simplest level, an account holder might begin making international funds transfers to high-risk countries related to Syria, such as Turkey, Lebanon or Jordan, for no apparent business or personal reason. Or an individual might buy an airline ticket to a popular summer tourist destination close to the Syrian border at an unusual time of year.

This paper draws on interviews conducted over the past twelve months with members of the financial-services industry, individuals operating in the Syrian–Turkish border region,[9] and government officials, as well as a desktop review of social-media sources such as Twitter and Facebook and websites such as Ask.fm and JustPaste.it that have become popular with those seeking related advice. Based on this information, this Occasional Paper argues that, within the limits of data privacy, an intelligent and intelligence-led relationship between governmental authorities and the financial-services industry could play a valuable contributing role in the more timely and effective identification of FTFs.

In considering this hypothesis, this paper is laid out as follows. It begins with a brief history of the foreign-fighter phenomenon in general, the emergence of insurgent groups in Syria and Iraq since 2011, and the appeal they hold for FTFs. It will then review the various profiles of those who travel from Western states to fight with these groups, their motivations and means of travel. It will also provide an overview of the advice given to aspiring travellers, particularly as it relates to travel, money and identity security, as well as considering the current international response to this phenomenon along with the wider issue of Daesh (also known as the Islamic State of Iraq and Syria, ISIS) financing. The paper will then study the role that FININT and the financial-services industry could play in enhancing these response efforts, considering views from within the financial-services industry and government authorities.

In September 2014, the UN Security Council urged UN member states to:[10]

> [P]revent the travel of foreign terrorist fighters from or through their territories, including through *increased sharing of information for the purpose of identifying foreign terrorist fighters*, the sharing and adoption of best practices, and improved understanding of the patterns of travel by

9. Interviews conducted via Skype and telephone.
10. UN Security Council Resolution 2178 (2014), p. 6. Emphasis added.

> foreign terrorist fighters, and for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law.

In addition, a recent FATF report acknowledges that more work needs to be done 'to develop red-flags to better identify the funding mechanisms FTFs utilize' and calls for 'greater domestic cooperation among AML/CFT [anti-money laundering and countering the financing of terrorism] bodies and other authorities'.[11] Including financial institutions in that work is clearly critical to the success and maximisation of these efforts.

Whilst it would be naïve to suggest that financial institutions have the ability to produce a form of financial 'minority report', the data they can access in tackling fraud and other financial crime is immense. Engagement between authorities and banks in exploiting this capability for security purposes remains limited. It thus seems likely that working in conjunction with intelligence services, financial institutions – if properly empowered – could significantly enhance the global effort to disrupt terrorism. At present the sector is an underutilised resource.

Before progressing, it is important to note that this analysis addresses the challenges posed by fighters travelling from Western nations to join designated terrorist organisations whilst acknowledging that a significant majority of the foreign fighters in Syria have travelled to the region from Arab countries and that a small number of Westerners have also travelled to fight with groups such as Kurdish *peshmerga* forces.

11. FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)', February 2015, p. 36, <http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf>, accessed 11 June 2015.

I. Foreign Fighters: A Time-Honoured Profession

The attraction of individuals from across the globe to fight for foreign causes is an ancient calling, from the Knights Templar to the more-than 5,000 unoccupied British soldiers recruited after the Napoleonic Wars by Simón Bolívar to his wars of national liberation in South America,[1] to those, like poet Lord Byron and author George Orwell, drawn respectively to fight in Greece for independence from the Ottoman Empire in the 1820s and against Franco in Spain in the late 1930s.[2]

Although the involvement of foreign fighters in jihadi conflicts seems commonplace now, such travelling foreign fighters – individuals who are generally defined as those who have travelled to fight in a conflict with which they have no direct link other than religious affinity[3] – were rare in the Muslim world before 1980.[4] Given the experience of the previous thirty years, however, in 2010 Hegghammer prophetically wrote that 'the next time a major conflict erupts in the Muslim world, expect to see foreign fighters again'.[5] Furthermore, in his view, jihad-inspired foreign fighters threaten the national security of their home states because 'volunteering for war is the principal stepping-stone for individual involvement in more extreme forms of militancy'.[6]

The UK's independent reviewer of terrorism legislation has likewise cautioned that:[7]

> The travel of UK nationals overseas to engage in jihad presents a number of potential threats to the UK, both while these fighters are overseas and on their return to the UK. The nature of these threats can differ, depending on the country in which they are fighting or the terrorist group which is hosting them, but there are a number of common themes. While overseas, these fighters can help terrorist groups develop their external attack capability by providing links with extremist networks in the UK and information about potential targets and the operating environment. In

1. David Malet, *Foreign Fighters: Transnational Identity in Civil Conflicts* (New York, NY: Oxford University Press, 2013), pp. 34–35.
2. See George Orwell's *Homage to Catalonia* (London: Secker and Warburg, 1938) for his personal account of his experiences as a soldier fighting in the Spanish Civil War from December 1936 to June 1937.
3. Thomas Hegghammer, 'The Rise of Muslim Foreign Fighters: Islam and the Globalization of Jihad', *International Security* (Vol. 35, No. 3, Winter 2010/11), p. 53.
4. *Ibid.*, p. 53.
5. *Ibid.*, p. 91.
6. *Ibid.*, p. 53.
7. David Anderson, *The Terrorism Acts in 2012: Report of the Independent Reviewer on the Operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006*, Independent Reviewer of Terrorism Legislation (London: The Stationery Office, 2013), p. 29.

> addition to English language skills which can help these groups with media outreach, some foreign fighters may also have other specialist skills (e.g. scientific, IT) that can help to strengthen the capability of these groups. The intelligence services have also seen foreign fighters attempt to direct operations against UK interests abroad.

Hegghammer's research has found that, on average, one in nine foreign fighters has returned home to take part in a domestic terror plot and that plots involving foreign fighters are more likely to reach execution, with double the likelihood the plot will have a lethal impact.[8] This potential for so-called 'blowback' has for some time worried security officials. For example, four of the five terrorist plots disrupted in the UK in the period 2010–12 involved individuals who had travelled to the Federally Administered Tribal Areas of Pakistan for training.[9] In March 2014, it was reported that more than half of the UK's Security Service's investigations involved Britons who had joined the conflict in Syria;[10] and according to ICSR, between 10 and 30 per cent of foreign fighters in Syria and Iraq have already left the conflict, either returning home or being stuck in transit countries. ICSR further notes that the number of foreign fighters in Syria and Iraq now exceeds the total number in the decade-long Afghanistan conflict in the 1980s.[11] Table 1, taken from ICSR's contribution to the 2015 'Munich Security Report', highlights the extent and breadth of foreign-fighter participation in the conflict in Syria and Iraq.

The extent to which the conflict in Syria and Iraq has attracted foreign fighters, combined with the attendant fears of blowback caused by those returning home, has created real urgency for the security authorities in identifying individuals who have travelled to the conflict zone and enhancing efforts to identify and prevent from travelling those that may be planning to do so. This work is all the more challenging because Syria is relatively easy to reach from a wide range of European and Arab countries in comparison with previous jihadi theatres such as Somalia and Afghanistan. The prevalence of budget-airline flights from many European capitals to Turkey has led some to dub this current conflict 'Easy Jihad',[12] with flights from across Europe to the

8. Thomas Hegghammer, 'Should I Stay or Should I Go? Explaining Variation in Western Jihadists' Choice between Domestic and Foreign Fighting', *American Political Science Review* (No. 107, February 2013).
9. Anderson, *The Terrorism Acts in 2012*, p. 29.
10. Sam Jones, 'MI5 Focuses on British Jihadists Returning from Syria', *Financial Times*, 14 March 2014.
11. Peter R Neumann, 'Foreign Fighter Total in Syria/Iraq Now Exceeds 20,000; Surpasses Afghanistan Conflict in the 1980s', ICSR, 26 January 2015, <http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/>, accessed 12 June 2015.
12. Sergei Boeke and Daan Weggemans, 'Destination Jihad: Why Syria and Not Mali', International Centre for Counter-Terrorism – The Hague, <http://icct.nl/publication/destination-jihad-why-syria-and-not-mali/>, accessed 17 June 2015.

Table 1: Foreign-Fighter Participation in Syria and Iraq.

Western Europe			Other Countries			
Country	**Estimate**	**Per capita***	**Country**	**Estimate**	**Country**	**Estimate**
Austria	100–50	17	Afghanistan	50	Morocco	1,500
Belgium	440	40	Albania	90	New Zealand	6
Denmark	100–50	27	Algeria	200	Pakistan	500
Finland	50–70	13	Australia	100–250	Qatar	15
France	1,200	18	Bahrain	12	Russia	800–1,500
Germany	500–600	7.5	Bosnia	330	Saudi Arabia	1,500–2,500
Ireland	30	7	Canada	100	Serbia	50–70
Italy	80	1.5	China	300	Somalia	70
Netherlands	200–50	14.5	Egypt	360	Sudan	100
Norway	60	12	Israel/Palestinian Territories	120	Tajikistan	190
Spain	50–100	2	Jordan	1,500	Turkey	600
Sweden	150–80	19	Kazakhstan	250	Turkmenistan	360
Switzerland	40	5	Kosovo	100–50	Tunisia	1,500–3,000
UK	500–600	9.5	Kuwait	70	Ukraine	50
			Kyrgyzstan	100	UAE	15
			Lebanon	900	USA	100
			Libya	600	Uzbekistan	500
			Macedonia	12	Yemen	110

*Up to; per million of population.

Source: ICSR contribution to 2015 'Munich Security Report'; see Peter R Neumann, 'Foreign Fighter Total in Syria/Iraq Now Exceeds 20,000; Surpasses Afghanistan Conflict in the 1980s', ICSR, 26 January 2015, <http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/>, accessed 12 June 2015.

Turkish–Syrian border costing little more than €300. For half that price, a Eurolines coach will take you from Frankfurt to Istanbul. Travel to join extremist Islamist groups such as Daesh and Jabhat Al-Nusra based in northern Syria could thus not be easier, more 'everyday' and more convenient. A dawn flight from London could deliver you to the battlezone in time for the *Isha'a* prayer at the end of the day. However, whilst the ease with which the conflict zone can be reached represents a threat and a challenge for international security authorities, it also creates an identification opportunity as travellers plan their travel from and pass through advanced economies where developed-world electronic banking is available and thus financial footprints are easily left.

Before considering the profile and motivations of the individuals most likely to make this journey, this paper will first review the groups that fighters are most likely to join, their ideologies and their appeal.

II. The Emergence of Insurgent Groups in Syria and Iraq

The turmoil that swept through the Arab world in early 2011, toppling the regimes in Tunisia and Egypt, reached Syria in March 2011. There, protests and demands for reform centred on the southern town of Deraa following the arrest and torture of teenagers who painted revolutionary slogans on a school wall. The Assad regime's response was brutal, killing many of the anti-government street protesters and triggering a hardening and arming of protests across the country as rebel brigades were formed and the country descended into civil war. As the conflict developed, private donations flowed in from neighbouring states, fuelling the increasingly sectarian nature of the fighting.[1] Whilst some funding reached the more moderate fighting groups under the banner of the Free Syrian Army, a significant proportion found its way to Islamist and jihadist groups, fuelling an escalation in the sectarian violence. Until 2014, the primary groups espousing strongly held Islamist and jihadist views were Ahrar Al-Sham and Jabhat Al-Nusra, a splinter of Islamic State of Iraq (ISI) which emerged in early 2012 when it was sent into the country from Iraq by ISI leader Abu Bakr Al-Baghdadi to capitalise on the developing chaos.

Following tensions between ISI and Jabhat Al-Nusra during 2013, as Al-Baghdadi sought to control both groups and unite them under the banner of the Islamic State of Iraq and Syria (ISIS) in contravention of the direction of Al-Qa'ida's leadership, Al-Qa'ida disaffiliated itself from ISI in February 2014.[2] ISI fighters now surged across northern Iraq, capturing border crossings, and into Syria, rapidly taking control of key commercial and population hubs including oil fields and refineries. In June 2014 the group declared a caliphate, renaming itself 'Islamic State'. In just a few short months, despite being dismissed by President Obama as 'a jayvee [junior varsity] team' in January 2014,[3] Daesh had become, in the words of former US Secretary of Defense Chuck Hagel, 'as sophisticated and well-funded as any group that we have seen. They're beyond just a terrorist group … they are tremendously well funded'.[4] Of course, the reality is that Daesh is not new; it is simply the latest incarnation of an insurgency that stretches back over a decade

1. For details of the role played by private donations in the conflict in Syria, see Elizabeth Dickenson, 'Playing with Fire: Why Private Gulf Financing for Syria's Extremist Rebels Risks Igniting Sectarian Conflict at Home', Analysis Paper No. 16, Brookings Institution, December 2013.
2. Aaron Y Zelin, 'The War between ISIS and Al-Qaeda for Supremacy of the Global Jihadist Movement', Research Notes No. 20, Washington Institute for Near East Policy, 2014, p. 3.
3. David Remnick, 'Going the Distance', *New Yorker*, 27 January 2014.
4. Spencer Ackerman, '"Apocalyptic" ISIS Beyond Anything We've Seen, Say US Defence Chiefs', *Guardian*, 22 August 2014.

and first came to prominence under the brutal leadership of Abu Musab Al-Zarqawi following the US-led invasion of Iraq in 2003.

Against this background – and with Daesh garnering abundant finance and territory, whilst rapidly becoming the dominant and most extreme force in the conflict – foreign fighters from across both the Arab and Western worlds streamed to join what many saw as an opportunity to take part in, and die as a martyr for, an 'end-of-days' battle in the defence of Islam, and to help Muslims under attack from the Assad regime. One such fighter, interviewed by the BBC, provides a typical explanation from that time in Daesh's development. Abu Muhadjar explained that:[5]

> There's many reasons [*sic*] made me leave my life and come here. The first is religious reasons – due to the fact that it's upon every single Muslim to protect Muslim lands and blood of Muslims if it's been transgressed upon. Second is humanitarian reasons – alongside of my fighting I tend to do aid work as well.

Whilst other groups such as Jabhat Al-Nusra received some FTFs, the vast majority were accepted by Daesh.

For the international community, this congregation of like-minded and extremist individuals posed a serious, transnational threat. As Nigel Inkster, director of transnational threats and political risk at the International Institute for Strategic Studies, noted to the UK Home Affairs Committee:[6]

> [T]he real worry about Syria is that it has the potential to become the crucible for a new generation of international jihadists, rather in the way as happened with those who took part in the anti-Soviet jihad in the 1980s, that they become a kind of band of brothers, united by shared experiences, shared outlooks, shared ideology, and that they then move on looking for new forms of jihad to undertake, one of which could well consist of attacks in countries such as the UK.

For many, Daesh and its newly declared caliphate provide a calling too strong to resist, and the need to travel to the conflict represents little impediment to answering that call.

5. Jenny Cuffe, 'Who Are the British Jihadists in Syria', *BBC News*, 15 October 2013.
6. House of Commons Home Affairs Committee, 'Counter-Terrorism', Seventeenth Report of Session 2013–14, HC 231, 9 May 2014, p. 19, <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf>, accessed 12 June 2015.

III. Who Travels and Why?

Just as the ungoverned space of Afghanistan in the 1990s provided the necessary sanctuary for the training of foreign fighters in paramilitary and other key terrorist skills such as bomb-making, so Syria has likewise emerged as an environment to which, encouraged by the siren call of jihad, foreign fighters are drawn. The Daesh magazine *Dabiq* calls on Muslims to make *hijrah* – the path to jihad – to the caliphate that the group has declared across Syria and Iraq, warning that 'abandoning *hijrah* … is a dangerous matter' that also reveals an individual as 'being a hypocritical spectator'.[1]

So who are the individuals who are drawn to the self-styled caliphate? What sort of person 'lives in the West amongst the *kuffar* [non-believers] for years, spends hours on the Internet, read[ing] news and posts on forums',[2] and then decides to turn his or her back on his or her former life and travel to fight in Syria and Iraq? Identifying profiles of those making this journey is an important preliminary step which can inform the pre-emptive intelligence that security services might provide to the financial-services industry.

According to the Soufan Group,[3] the typical age range of those known to have travelled to Syria or those who have revealed themselves as foreign fighters is 18–29, with reported examples of some as young as 15–17 years old travelling as well as others in their thirties. Most are male, although an increasing number of women are making the journey (the estimate for EU member states is put as high as 18 per cent).[4] Most of the individuals who arrive, particularly those from Western states, have no previous military training or fighting experience; in contrast, many of the Arab fighters, as well as those from Chechnya, are highly experienced. The Soufan Group also reports that an average of 6 per cent of the fighters from EU countries are converts to Islam, few have any connection with Syria, and many are second- or third-generation immigrants in their home countries.[5]

The motivations for travel vary. Many were initially drawn by the desire to fight Assad and bring to a halt his indiscriminate killing of the Syrian people, something the international community had failed to do. Others are drawn by the purpose that jihad seemingly brings to their lives, lives that are often disaffected in the West, and which they believe will be better spent fighting in what is viewed by many as the defining battle for Muslims as they defeat

1. *Dabiq* (No. 3, 2014), p. 27.
2. *Ibid.*
3. Richard Barrett, 'Foreign Fighters in Syria', Soufan Group, June 2014, p. 16, <http://soufangroup.com/wp-content/uploads/2014/06/TSG-Foreign-Fighters-in-Syria.pdf>, accessed 12 June 2015.
4. *Ibid.*, p. 16.
5. *Ibid.*

the infidels once and for all in a predicted 'Day of Judgment'.[6] The language used by Daesh's slick media operation taps into this desire to join the ultimate battle, coining 'youth speak' language and posing questions such as 'YODO: You Only Die Once. Why not make it martyrdom?'[7] However, perhaps the most unifying factor amongst Western foreign fighters is the possibility of living somewhere governed solely by the teachings of Islam. Many recruits from Western countries have only a limited grasp of Islam, but the clear direction provided by Sharia Law and the contrast with what they perceive as the decadence of Western nations provide significant motivation. In the view of Richard Barrett, travelling to Syria has 'mostly to do with the search for identity … coupled with a search for belonging and purpose. The Islamic State offers all that and empowers the individual within a collective. It does not judge and accepts all with no concern about their past. This can be very appealing for people who think that they washed up on the wrong shore'.[8] Of course, the reality is often far from these travellers' expectations.

Whilst some fighters profess no interest in returning to their homes in the West – or if they do, have no expressed intent to return in order to carry out terrorist attacks[9] – a range of videos, articles and speeches threaten quite the reverse. The British fighter,[10] so-called 'Jihadi John', seemingly responsible for the majority of the brutal murders of Western journalists and aid workers, has vowed to President Obama to 'begin to slaughter your people on your streets'.[11] In September 2014, Daesh spokesman Abu Mohammed Al-Adnani threatened citizens of all countries involved in attacking the group, encouraging Muslims living in these countries to kill 'disbelievers … in any manner or way however it may be',[12] and warning Western citizens that they 'will not feel secure even in [their] bedrooms' and that they 'will

6. William McCants, 'ISIS Fantasies of an Apocalyptic Showdown in Northern Syria', Brookings Institution, 3 October 2014, <http://www.brookings.edu/blogs/markaz/posts/2014/10/03-isis-apocalyptic-showdown-syria-mccants>, accessed 12 June 2015.
7. *National,* '20,000 Foreign Fighters Head to Syria, US Intel Shows', 11 February 2015, <http://www.thenational.ae/world/middle-east/20000-foreign-fighters-head-to-syria-us-intel-shows>, accessed 12 June 2015.
8. Richard Barrett quoted in Mehdi Hasan, 'How Islamic is Islamic State?', *New Statesman*, 10 March 2015.
9. See, for example, the interview with a Dutch foreign fighter discussed in Robert Mackey, 'A Dutch Jihadist in Syria Speaks, and Blogs', The Lede: New York Times News Blog, 29 January 2014, <http://thelede.blogs.nytimes.com/2014/01/29/a-dutch-jihadist-in-syria-speaks-and-blogs/>, accessed 12 June 2015.
10. In February 2015, Jihadi John was revealed as Mohammed Emwazi, a Kuwaiti-born British man from west London. See *BBC News*, '"Jihadi John" Named as Mohammed Emwazi from London', 26 February 2015.
11. Ben Farmer, 'Isil Threatens Slaughter in the Streets of the West', *Daily Telegraph*, 16 November 2014.
12. Helen Davidson, 'Isis Instructs Followers to Kill Australians, and Other "Disbelievers"', *Guardian*, 23 September 2014.

pay the price when this crusade … collapses'.[13] The fourth issue of Daesh's *Dabiq* magazine urged Muslims to 'Rush to support your state'; it further stated that 'it is very important that attacks take place in every country that has entered into the alliance against Islamic State' and that 'the citizens of crusader nations should be targeted wherever they can be found', whilst also warning against the 'analysis paralysis' that comes from over-engineering an attack. Furthermore, a Muslim 'should be pleased to meet his Lord even if with just one dead *kafir*'s [infidel's] name written on his scroll of deeds' and should thus 'get out of his house, find a crusader, and kill him', attributing his actions to the so-called Islamic State.[14]

Together, the historical, statistical analysis of Hegghammer and the increasingly numerous examples of the murderous motivation Daesh allegedly provides to the likes of Mehdi Nemmouche, who return home to mount attacks in the West, underline the critical importance of identifying and stopping those who are considering travelling to Syria, as well as tracking those who are travelling or who have travelled to Syria, to ensure they can be interdicted prior to arrival in Syria or before returning to their home country. As the recent case of three East London schoolgirls who travelled to Syria during their school holiday reveals, efforts to achieve these goals still fall short of any objective measure of success – success that, this paper argues, could be enhanced by the greater use of financial intelligence and partnership between the security authorities and the financial-services industry.

13. Damien McElroy and Philip Sherwell, 'Islamic State: "You are Not Even Safe in Your Bedrooms"', *Daily Telegraph*, 22 September 2014.
14. *Dabiq* (No. 4, 2014), p. 44.

IV. International Efforts to Disrupt Finance and Fighters

The blizzard of UN Security Council resolutions aimed at tackling terrorist financing in general and specific issues related to Daesh, other designated terrorist groups operating across Syria and Iraq such as Jabhat Al-Nusra, and foreign terrorist fighters is impressive.[1] The regularity with which resolutions have been passed is one indication of the urgency with which the Security Council is treating the conflict in Syria and Iraq and its associated consequences. It is also an indication of the apparent sense of powerlessness felt by the Security Council, seemingly unable to affect the course of the conflict in any meaningful way.

As underlined by the continuing passing of Security Council resolutions, countering the financing of Daesh is a cornerstone of the efforts by the international community to restrict the group. Since the world awoke to the threat posed by Daesh, it is the group's financial strength that has drawn most attention. The campaign of airstrikes has sought to destroy and disrupt the refining and smuggling of oil; regional neighbours have been encouraged to curtail the flow of private donations to designated groups; and dealers in antiquities are being pressed to ensure looted artefacts are not traded. Anecdotal reporting suggests that the financial squeeze being placed on Daesh is certainly affecting those living in areas controlled by the group, as services and fuel supplies are in increasingly short supply; however, whether these efforts are reducing the threat posed by Daesh remains yet to be seen.

In September 2014, as the bombs and missiles started to fall on Daesh and other jihadi groups in Iraq and Syria, the UN Security Council passed Resolution 2178, which condemned violent extremism and underscored the need to prevent travel by and support for FTFs. The passing of the resolution was an acknowledgment by the international community that FTFs represent an 'acute and growing threat'. Furthermore, along with the aims of 'addressing underlying factors', 'preventing radicalisation' and 'countering violent extremism', the UN Security Council called for the 'inhibiting [of] foreign terrorist fighter travel [and disruption of] financial support'.[2] Yet despite the focus of the resolution on financial support, beyond the usual and oft-repeated calls to criminalise terrorist financing and bring to justice those who finance terrorist acts, nothing new was offered. This contrasted sharply with the measures proposed to prevent physical travel, such as controlling the issue of identity papers and preventing counterfeiting,

1. See, for example, in the past eighteen months UN Security Council Resolutions 2133 (2014), 2160 (2014), 2161 (2014), 2170 (2014), 2178 (2014), 2195 (2014) and 2199 (2015).
2. UN Security Council Resolution 2178 (2014).

forgery or fraudulent use of travel documents, and recommending traveller risk assessment and screening.

Particularly striking was the call made upon airlines to join the effort to detect and disrupt designated individuals. Just as airlines hold valuable data about their passengers, so banks can reveal considerable intelligence with regards to the whereabouts, activities, and intentions of their account and card holders. Why was this valuable resource apparently overlooked by the UN Security Council when the application of FININT is proven to contribute considerably to national and international security?

V. ‘As-salam alaikum my brother. How much money should I bring?’

Online radicalisation and recruitment techniques used by Daesh and other jihadi groups have received considerable and increasing media attention as the conflict in Syria has continued. As a number of analysts have noted, ‘Syria’s [conflict] has been the most socially mediated civil conflict in history’.[1] One specific purpose for which online channels have been used is to offer financial and travel advice including which hotels and border-crossing points to use, how much money to bring, services provided by Daesh, visa requirements, and even whether wifi and contact lenses are available. The international community has sought, in vain, to disrupt and remove these sources from the Internet. As quickly as one source is shut down, it reappears via a new account. For example, in February 2015, UK counter-terrorism police adjudged an amateurish although informative travel guide circulating on the Internet for those seeking to join Daesh to be ‘a threat’.[2] Links on sources such as JustPaste.it and Scribd.com were removed, but within twenty-four hours the guide was once again circulating on Twitter.

There are many examples of foreign fighters already in Syria who are advising potential recruits via the Internet and social media, answering their questions about the best means of reaching the ‘Islamic State’ undetected by authorities. One fighter believed already to be in Syria and calling himself Abu Abdullah Al-Britani advises that those travelling to join the fight should make sure they have enough money to cover staying in Turkey in case transit to Syria is delayed. He further advises that travellers should avoid raising the suspicion of airport authorities by carrying no more than £3,000, and if challenged to simply say they are taking an ‘extravagant holiday’.[3] Daesh itself also offers financial advice in its *Dabiq* magazine to those ‘embarking upon *Hijrah*’ to the caliphate, reassuring travellers not to ‘worry about money or accommodations [as] there are plenty of homes and resources to cover you and your family’.[4]

Information is also provided for those wondering how much money they will need for living expenses. Some responses aim to reassure: ‘Not much several hundred, u dnt need much, u get wages here, u get food provided and place

1. Marc Lynch, Deen Freelon and Sean Aday, *Syria’s Socially Mediated Civil War*, Peaceworks No. 91 (Washington, DC: United States Institute of Peace, 2014).
2. Constanze Letch, Carmen Fishwick and Vikram Dodd, ‘UK Police Move to Take Down Islamic State How-To from Internet’, *Guardian*, 26 February 2015.
3. John Hall, ‘“Come and Get Your AK47, Your Grenades and Your Vest Pack”: British ISIS Fighter Lures Underage Jihadist Away from His Parents with Travel Advice on Reaching Middle East’, *MailOnline*, 24 June 2014.
4. *Dabiq* (No. 3, 2014), p. 33.

to stay [*sic*]',[5] says one, whilst another agrees, 'nothing really at all [– all] is provided. All that's needed is to pay towards getting here'.[6] Others provide answers to more specific financial questions such as whether weapons or clothing have to be paid for. 'No' is the response, 'we get weapons from Dawlatul-Islamiyyah [referring to Islamic State]', but if a fighter wants to buy a specific weapon he is advised that a modern AKM Kalashnikov assault rifle costs US$1,200, older AK-47s cost even more. Likewise, clothing is provided by Daesh but can also be bought and even tailored for the aspiring jihadist.[7]

Box 2: Travel Advice Available Online.

Plenty of practical, open-source travel and financial advice is available online for the would-be jihadist. Below is a selection of reproduced screenshots that have been collected by ICSR at King's College London and generously shared with the research team for this paper.

akhi, if I am bringing Money what is the safest way to bring it, I mean how if I am bringing a decent amount?

Just bring it with u and say u goin on a extravagant holiday or something, I think they will only ask u questions abou money laundering if u have over 3k or sumin, but check that info out

about 15 hours ago

Assalmaualkum, i have question with regards to money. How do i change Canadian money into Syrian money. Do they have exchange beureus in Syria. JZK . (first time traveliling)

(Asked by Anonymous)

Wa'alaykum al-salām wa rahmatulLah wa barakātuh.
Change your Canadian dollars into US dollars before you leave. You will be able to change your money in Shām but USD is your safest bet as people might be reluctant to exchange other currencies.
wAllahu a'lam

5. John Hall, '"U Dnt Need Much, U Get Wages Here, U Get Food Provided and Place to Stay": The Rough Travel Guide British ISIS Fighters are Using to Lure Fellow Britons in to Waging Jihad in Iraq', *MailOnline*, 18 June 2014.
6. Joanna Paraszczuk, 'The Frequently Asked Questions of Aspiring Jihadists', *Atlantic*, 12 November 2014.
7. *Ibid.*

ahki i need to know something quick, do i need a lot of money when i come there because i have only enough for the plane ticket.

abu-dujanna-as-somalee:

You will be taken care of here :) but try bring some spends

Posted 4 days ago

3 notes

can we only exchange US money in Syria or even other money I exchange british money here :p u do alot here akhi :p

9 days ago

Assalamualaykum brother...is there any service in shaam where people can send /transfer money from shaam to anywhere in the world? example western union..jazakallahu khair

wsalaam there is brother

2 days ago

Where do you get the money from?

Generous muslims abroad who makes their jihad a financial jihad. may Allah swt reward them

4 days ago

1 person likes this

assalmualkum brother, jazakullah for answering question bout money and internet, I havent any traveling and i'm underage but what do you mean with no worries about money. honestly I don't know how to change money into tukish or syrian money. How does it work? I can't ask my parents or they will now

Akhi if you have $ or £ then u fine, any other currency exchange it to $ or £ before u get here and in sha Allah u will be fine

3 days ago

how much money did u come with ?

not much several hundred, trus u dnt need much, u get wages here, u get food provided and place to stay, when u get married in sha Allah u will get money for wife and kids and if u dnt have a house isis wilk give u one and if not that they give u money to rent,
Alhamdulilah

7 days ago

Where do the mujahideen get their money From?

many revenues, business, oil rigs, gas, petrol a d diesel, ghanayam, funding..alhamdulilah all from Allah azza wajjal

12 days ago

1 person likes this

But who give to Dawlah? Did Dawlah Get Revenue from Occupied places... Or saudi Qatari Shaikhs provided the money...? Baz

we get revenue from jihad, some funds come from abroad but from halal sources, most of our revenue is from occupied places

about 22 hours ago

As-salam alaikum my brother. How much money should I bring?

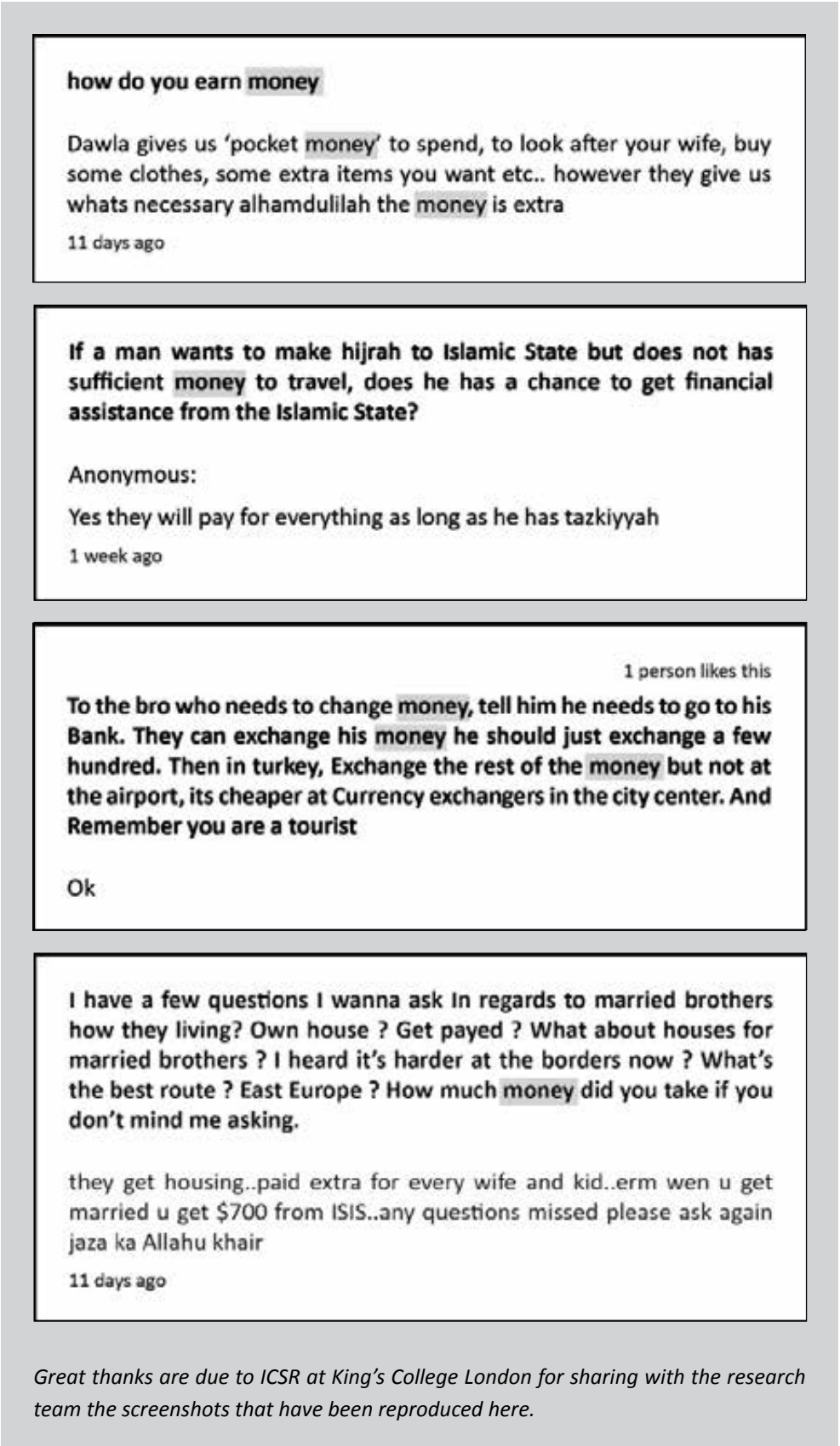
Enough for ticket and couple more hundred

6 days ago

how much money you get for fighting in Syria?

None we get a smal wage just for personal neccesities which u dnt really need, if I was lppking for money I wouldve stayed in the west, we lookin to please our lord and attain a succesful status in the hereafter bithinillah

5 days ago



how do you earn money

Dawla gives us 'pocket money' to spend, to look after your wife, buy some clothes, some extra items you want etc.. however they give us whats necessary alhamdulilah the money is extra

11 days ago

If a man wants to make hijrah to Islamic State but does not has sufficient money to travel, does he has a chance to get financial assistance from the Islamic State?

Anonymous:

Yes they will pay for everything as long as he has tazkiyyah

1 week ago

1 person likes this

To the bro who needs to change money, tell him he needs to go to his Bank. They can exchange his money he should just exchange a few hundred. Then in turkey, Exchange the rest of the money but not at the airport, its cheaper at Currency exchangers in the city center. And Remember you are a tourist

Ok

I have a few questions I wanna ask In regards to married brothers how they living? Own house ? Get payed ? What about houses for married brothers ? I heard it's harder at the borders now ? What's the best route ? East Europe ? How much money did you take if you don't mind me asking.

they get housing..paid extra for every wife and kid..erm wen u get married u get $700 from ISIS..any questions missed please ask again jaza ka Allahu khair

11 days ago

Great thanks are due to ICSR at King's College London for sharing with the research team the screenshots that have been reproduced here.

Travel to Syria is simple. Given the availability of flights and buses from European cities to neighbouring Turkey, planning a trip is straightforward – Turkey has visa-free relations with at least seventy countries and a simple e-visa scheme for those who do require visas.[8] As noted in Chapter I, despite the posts on jihadi fora cautioning aspiring fighters to plan their journey carefully to avoid arousing suspicions – for example, making intermediate stops, taking indirect routes, travelling with aid convoys,[9] or even travelling aboard cruise ships[10] – reaching the Syrian border is relatively cheap and trouble free. Flights from across Europe to regional towns such as Hatay and Gaziantep or the beach resort of Antalya cost €300–500; buses cost even less.

However, although travel to the region is quick, straightforward and relatively cheap, aspiring fighters still need money to pay for the journey and to sustain themselves en route, even if they are assured that all needs will be taken care of once they arrive in Syria.

The Internet may be a valuable tool for recruitment and advice, 'chock full of propaganda from Syrian jihadi groups as well as practical travel advice for budding foreign fighters'; however, it is also a liability for travellers and fighters as it increases the ability of government security agencies to locate and detain users.[11] As the next chapter will explore, use of financial services by (would-be) jihadis can be similarly revealing.

8. For specific details see Republic of Turkey, Ministry of Foreign Affairs, 'Visa Information for Foreigners', <http://www.mfa.gov.tr/visa-information-for-foreigners.en.mfa>, accessed 12 June 2015.
9. Charity Commission, 'Syria and Aid Convoys', 21 February 2014, <https://www.gov.uk/government/news/syria-and-aid-convoys>, accessed 17 June 2015.
10. *BBC News*, 'Jihadists "Using Cruise Ships" to Reach Middle East War Zones', 7 November 2014.
11. Thomas Hegghammer, 'Syria's Foreign Fighters', ForeignPolicy.com, 9 December 2013.

VI. The Role FININT Can Play

What is clear from a review of the literature pertaining to the FTF phenomenon is that when it comes to identifying foreign fighters, the authorities need to continually assess whether the most effective tools are being used. As has been noted, 'everyone working on this phenomenon should be aware of the constant need to check the facts and test the assumptions and tools that are available and, if needed, look for new ones, in order to gain more insight into the constantly evolving phenomenon of European jihadi foreign fighters'.[1] It is in this context – and consistent with the FATF view that 'the effectiveness of authorities at both detecting and investigating terrorist activity is significantly enhanced when counter-terrorist intelligence and financial information are used together'[2] – that this Occasional Paper argues that the role of the financial-services industry, previously underexploited, can contribute a fresh and insightful dimension to the intelligence picture of those that are travelling for jihad, thus assisting with their identification, the disruption of travel and prosecution.

Before elaborating on this argument, it is important first to understand both the way in which the financial-services industry, specifically banks, monitor transactions and the legal framework within which this is generally done, acknowledging that country-specific regulations often apply.

Banks and Transaction Monitoring

Financial institutions undertake extensive transaction monitoring as they seek to protect both themselves and their account holders from becoming victims of fraud and other forms of financial crime. A range of so-called 'red-flag' activities alert banks to the possibility that some form of financial crime is in progress.[3]

As the UK's Joint Money Laundering Steering Group (JMLSG) explains:[4]

> Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money

1. Edwin Bakker, Christophe Paulussen and Eva Entenmann, 'Dealing with European Foreign Fighters in Syria: Governance Challenges and Legal Implications', ICCT Research Paper, December 2013, p. 22.
2. FATF, 'Terrorist Financing', 2008, p. 4, <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf>, accessed 12 June 2015.
3. Red-flag activity refers to account-holder activity that is inconsistent with the account holder's typical activity or activity which reflects known concerns, such as transactions to certain high-risk countries, frequent near-simultaneous receipts and transfers, and other particular occurrences which financial institutions have learnt to be symbolic of potentially illicit activity.
4. Joint Money Laundering Steering Group, 'Prevention of Money Laundering/Combating Terrorist Financing', December 2011, p. 109, <http://www.jmlsg.org.uk/download/7324>, accessed 12 June 2015.

> laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime.

As it relates to the current conflict in Syria, the Australian government's financial intelligence unit (FIU), the Australian Transaction Reports and Analysis Centre (AUSTRAC), provides clear transaction monitoring-related guidance in its recent review of terrorism financing in Australia:[5]

> Australian financial institutions should ensure their transaction monitoring programs are dynamic and updated regularly to reflect current terrorism financing threats. In particular, Australian reporting entities should take into account international conflicts and tensions of concern to the Commonwealth Government because of their potential to affect Australia's terrorism risk environment. Currently:
>
> - funds sent to Syria and neighbouring countries warrant scrutiny for possible terrorism financing activity
> - transactions involving other countries facing insurgency or terrorist threats, such as Yemen and Somalia, or neighbouring countries with established financial sectors, may also involve terrorism financing risks.

Whilst a range of general and idiosyncratic activities might create monitoring 'red flags', these alerts are not by themselves evidence of criminal activity, but typically suggest that closer analysis is required in order to determine whether there is a reasonable business or legal rationale for the unusual activity.

The technology that supports transaction monitoring has evolved rapidly, supporting both rule-based and intelligent systems. The former is static and uses set criteria; the latter is more sophisticated and is capable of filtering transactions based on historical activity or in comparison to a defined peer group to determine inconsistencies or 'red flags'.[6] The key to effective transaction monitoring is thus knowledge of typical account activity against which deviations and inconsistencies can be mapped. Just as financial institutions undertake this analysis to protect themselves and their account holders from fraudulent activity based on this historical analysis, so, it would seem, could they conduct such analysis to identify activity that might be consistent with the financial footprints left by those travelling to fight with designated terrorist organisations.

---

5. Australian Transaction Reports and Analysis Centre, 'Terrorism Financing in Australia 2014', p. 22.
6. Red-flag activity is first reviewed within the financial institution so that a determination can be made as to whether or not a suspicious activity report should be filed with the relevant government authority.

Box 3: The FFIEC Guide to Activity Potentially Indicative of Terrorist Financing.

The US Federal Financial Institutions Examination Council (FFIEC)[1] provides a useful guide, summarised below, of potentially suspicious activity that may indicate terrorist financing.[2]

Activity Inconsistent with the Customer's Business

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (for example, countries designated by national authorities and the FATF as non-co-operative countries and territories)
- The stated occupation of the customer is not commensurate with the type or level of activity
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (for example, student, unemployed or self-employed)
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected
- Multiple personal and business accounts or the accounts of non-profit organisations or charities are used to collect and funnel funds to a small number of foreign beneficiaries

1. Federal Financial Institutions Examination Council (FFIEC), 'About the FFIEC', <http://www.ffiec.gov/about.htm>, accessed 16 June 2015.
2. FFIEC, 'Appendix F: Money Laundering and Terrorist Financing "Red Flags"', in 'FFIEC Banking Secrecy Act/Anti-Money Laundering Examination Manual', <https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_106.htm>, accessed 16 June 2015.

- Foreign-exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers either to locations with no apparent business connection with the customer or to higher-risk countries.

Other Transactions that Appear Unusual or Suspicious

- Transactions involving foreign-currency exchanges are followed within a short time by funds transfers to higher-risk locations
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations
- Banks from higher-risk locations open accounts
- Funds are sent or received via international transfers from or to higher-risk locations.

However, whereas financial institutions have a significant pool of experience on which to draw when tackling fraud and other forms of financial crime, they are less well equipped to identify activity consistent with FTFs unless supplied with typologies by those better informed, namely the security authorities.[7] It therefore seems plausible that with the assistance of the intelligence services, combinations of these 'red flags' could be used to help banks identify people travelling, or *planning* to travel, to join terrorist organisations such as Daesh. *Thematic* information could be provided to financial institutions by the intelligence and security authorities that might allow banks to adjust their transaction-monitoring systems and algorithms to identify more easily suspicious activity consistent with foreign fighters. Interviews conducted for the research on which this Occasional Paper is based have revealed a number of characteristics that are consistent with the financial activities of those who are planning to travel to Syria, are en route, or have already arrived there. Whilst these indicators are not unique to this type of traveller, they can potentially help inform the transaction monitoring undertaken by the financial-services industry.

7. Identifying activity consistent with FTFs is more challenging as it is, in the main, activity that is per se entirely legal, such as buying an airline ticket or withdrawing money from an ATM. Thus, intelligence input is needed in order to put a bank on notice that certain forms of inherently unsuspicious activity should be reported.

Examples gathered during research included combinations of account-holder age and gender, usage patterns involving the purchase of airline or long-distance bus tickets to certain key destinations, extended periods of account dormancy, noticeable changes in account usage, unusual use of remittance services, and ATM or credit-card usage in recognised 'hotspots', such as towns in southern Turkey or neighbourhoods of cities such as Istanbul where transit-travellers are known to congregate. Of course, none of these features is definitive, and the financial-services industry is rightly cautious of undertaking activity that might possibly be classed as 'profiling';[8] but the industry's automatic transaction-monitoring capabilities are significant and, at present, are underutilised. Thus, just as transaction monitoring might create an instant alert leading to a credit-card holder receiving a call or text confirming unusual credit-card usage, so these systems can be set to filter for other forms of notable or unusual behaviour.

Whilst banks and other financial institutions can make a 'best guess' of what characteristics might be consistent with foreign-fighter usage, partnership with the authorities has the potential to create a much more effective and informed picture. As Richard Barrett, the former co-ordinator of the UN Al-Qa'ida and Taliban Monitoring Team, has underlined, 'States cannot expect the private sector to have a better idea of what terrorist financing looks like than the states themselves'.[9]

It would therefore seem clear that the key to enhancing the ability of financial institutions to identify transactions that might indicate foreign-fighter-related activity is information sharing.

Partnership and Information Sharing

In most countries, the relationship between the security and law-enforcement authorities and the financial-services industry is transactional and generally one-sided. Law-enforcement agencies tend to engage with a financial institution following a specific event as part of their investigations. Those who have experienced this working relationship typically classify the partnership as 'good' and 'productive'. Yet outside a specific case-related dialogue, partnership is limited.

KPMG's triennial global anti-money laundering surveys published in both 2011 and 2014 highlight the core issues: banks desire more guidance from, and collaboration with, the authorities in meeting their AML/CTF obligations.[10]

8. A number of interviewees strongly emphasised this point.
9. Richard Barrett, 'Preventing the Financing of Terrorism', *Case Western Reserve Journal of International Law* (Vol. 44, No. 3, 2011), p. 730.
10. KPMG, 'Global Anti-Money Laundering Survey: How Banks are Facing Up to the Challenge', 2011, <https://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/Advisory/global-aml-survey-2011-main-

The one-way flow of information that typically exists is counterintuitive given that the governmental authorities are relying on the financial-services industry to form a front line in countering terrorism.

For many years, under most national laws and international standards addressing money laundering and terrorist financing, financial institutions – along with a range of other industry sectors such as lawyers, accountants, estate agents, and casinos that handle or enable the movement of significant sums of money and are thus vulnerable to abuse for money-laundering and terrorist-financing purposes – have been required to file SARs with their local FIU.[11] For example, in the year to September 2014, over 350,000 SARs were filed with the UK's National Crime Agency (NCA), the designated FIU for the UK – 300,000 of which came from banks or building societies.

Two issues are striking. First, given the volume of SARs submitted to national FIUs, it seems unlikely that they are able to process, utilise and investigate the increasing annual weight of filings. Secondly, how are filing institutions determining what is 'suspicious'? How do they know what information is of use to their FIU or are they simply filing SARs to avoid accusations of negligence in comparison to peers? The quality of SARs has a direct impact on the ability of law-enforcement agencies to disrupt financial crime and other forms of illicit finance; and the quality of the SARs is more often than not directly impacted by the extent to which the filing institution is made aware of current and specific threats by law-enforcement agencies.

As noted by the 9/11 Commission's 'Monograph on Terrorist Financing', terrorist-financing transactions are 'often small or consistent with the customer's profile … and seemingly innocuous',[12] elaborating further that:[13]

> [B]anks generally are unable to separate suspicious from legitimate transactions. The government, however, may have information that would

report.pdf>, accessed 16 June 2015; KPMG, 'Global Anti-Money Laundering Survey', 2014, <http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/global-anti-money-laundering-survey/Documents/global-anti-money-laundering-survey-v6.pdf>, accessed 19 June 2015.

11. Recommendation 20 from global standard-setter FATF states: 'If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)'. FATF, 'The FATF Recommendations', February 2012, p. 19, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf>, accessed 16 June 2015.
12. John Roth, Douglas Greenburg and Serena Wille, 'Monograph on Terrorist Financing', staff report to the National Commission on Terrorist Attacks upon the United States', 2004, p. 52, <http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf>, accessed 17 June 2015.
13. *Ibid.*

> enable banks to stop or track suspicious transactions. As a result, financial institutions can be most useful in the fight against terrorist financing by collecting accurate information about their customers and providing this information – pursuant to legal process – to aid in terrorism investigation. At the same time, the government should strive to provide as much unclassified information to financial institutions as possible.

Put simply, 'Although financial institutions lack information that can enable them to identify terrorists, they have information that can be absolutely vital in finding terrorists'.[14] The components necessary to empower banks to play this important counter-terrorism role are, in the main, absent.

Belatedly, in certain countries, work is being done to strengthen this weakness in national financial defences. In the UK, the Home Office and NCA have created the Financial Sector Forum and Joint Money Laundering Intelligence Taskforce (JMLIT) to bring law-enforcement and regulatory authorities together with the private sector in an effort to enhance information sharing. A recent interview with the director general of the NCA in the *London Evening Standard* revealed the progress this initiative is making, but it also underlined the legal challenges that data protection and privacy laws present; indeed, he admitted that 'Both the NCA and the banks expect to face legal challenges … from customers angry that details about their financial dealings have been given to the authorities'.[15]

Whilst information sharing by the law-enforcement and security authorities has the potential to enhance significantly the monitoring capabilities of the financial-services industry, the 9/11 Commission sounded a note of caution:[16]

> Providing intelligence about terrorist financing to bank personnel raises serious privacy and civil liberty issues. People may be named in intelligence reports, but many of the allegations within these reports are unproven … Turning these reports over to private citizens like bank personnel runs the risk that entirely unsubstantiated allegations may lead banks to shut customer accounts or take other adverse action.

Facilitating the sharing of information between the public and private sectors is not the only barrier that needs to be addressed. Whilst this paper is focused on the relationship between the public sector and the financial-

14. *Ibid.*, p. 58.
15. *London Evening Standard*, 'Crime in Banks "a Threat to National Security," Says NCA Boss Keith Bristow', 16 February 2015, <http://www.standard.co.uk/news/uk/crime-in-banks-a-threat-to-national-security-says-boss-of-national-crime-agency-10048870.html>, accessed 16 June 2015.
16. Roth, Greenburg and Wille, 'Monograph on Terrorist Financing', p. 64.

services industry, information-sharing barriers exist elsewhere too. Sharing information between national FIUs is challenging and laborious, despite the systems provided by Egmont, the global convener of FIUs,[17] and FIU.net, an information-sharing mechanism used by some FIUs within the EU; even sharing information *within* an individual bank can be restricted.

It is with the important warnings and concerns of the 9/11 Commission in mind that this paper will next consider the legal and privacy issues that are paramount in assessing the enhanced security role banks might play in partnership with the authorities.

Privacy and Data Protection

Calls for the financial-services industry to utilise its customers' data to provide financial intelligence as a means of contributing to the strategy to combat FTFs travelling to Syria and Iraq will quite rightly raise concerns and objections from privacy and civil-liberties groups. These concerns would fit into the ongoing public debate about intelligence agencies' increasing exploitation of ever-ubiquitous technology, given that 'globalisation and growing dependence on information technology in all spheres of society have led to a dramatic increase in the level of electronically compiled and transmitted personal data'.[18] For over a decade the UN has expressed concern regarding 'the ways in which counter-terrorist legislation adopted by governments might infringe on human rights and civil liberties'.[19] Others have also expressed concerns that excessive data gathering has now exceeded 'stated objectives by contributing to extra judicial security action'.[20] It is thus critical that an appreciation of data-privacy issues and the necessity of ensuring legality are maintained, in order to ensure that any intelligence gathering by the financial-services industry is proportionate, necessary and just.

17. The Egmont Group is an international network of FIUs set up in 1995 that aims to enhance communication, information sharing and training amongst its members as they support governmental AML/CTF efforts. As it relates to information sharing, Egmont's secure Internet system allows FIUs to communicate securely, requesting and sharing case information, and posting and assessing information on typologies, analytical tools and technological developments.
18. Ekaterina A Drozdova, 'Civil Liberties and Cyber Space', CISAC Report, August 2000, pp. 11–12, <http://fsi.stanford.edu/sites/default/files/drozdova.pdf>, accessed 16 June 2015.
19. Christopher C Joyner, 'The United Nations and Terrorism: Rethinking Legal Tensions between National Security, Human Rights, and Civil Liberties', *International Studies Perspectives* (Vol. 5, No. 3, August 2004), p. 243.
20. Marc Parker and Max Taylor, 'Financial Intelligence: A Price Worth Paying?', *Studies in Conflict and Terrorism* (Vol. 33, No. 11, 2010), pp. 949–59; see also commentary in Marieke de Goede, 'Risk, Preemption and Exception in the War on Terrorist Financing', in Louise Amoore and Marieke de Goede (eds), *Risk and the War on Terror* (Abingdon: Routledge, 2008).

Some privacy advocates argue that banks' use of customer data to generate FININT is overly intrusive. Indeed, even in the febrile environment following 9/11, the 9/11 Commission observed that 'despite [the attacks], it seems that privacy concerns will prevent anything remotely like these ideas [about technology being used to identify terrorists financially] from becoming reality in the foreseeable future'.[21] Others have argued that the UN must be concerned with developments about extending legislative powers 'because restrictions of fundamental freedoms for the sake of national security may be dangerous to the future of a democratic society'.[22] The 9/11 Commission also argued at the time that creating a situation where classified information is shared with banks 'cannot be justified by the minimal benefits that sharing classified information might produce',[23] believing that 'most intelligence on terrorist financing is not actionable … the intelligence tends to be limited and speculative'.[24] Assessing the question of what more can be done, the 9/11 Commission bluntly stated that 'sharing classified information with bank personnel' is 'a bad idea'.[25]

However, the 9/11 Commission importantly conceded that if the intelligence community develops patterns or trends regarding terrorists, these can legitimately be shared with financial institutions.[26] On the face of it, most FTF-related financial activity such as purchasing airline tickets, making ATM withdrawals, or sending and receiving funds appears entirely innocent. Intelligence indicating which forms of financial activity are consistent with current security threats can be invaluable for financial institutions. Thus, within the parameters of acceptable data-privacy restrictions, an intelligence relationship between the governmental authorities and the financial-services industry could be extremely effective in helping financial institutions interpret their vast quantities of data, thus providing actionable FININT in the effort to tackle the flow of FTFs attracted to Daesh. Privacy concerns rightly abound. Yet many observers often point to the fact that 'one of the most important findings of research on mass beliefs about democracy and civil liberties is the importance of context'.[27] Thus, privacy concerns need not be a barrier to the use of this potentially vital tool in combating the very real and significant threat posed by FTFs, but the value of this approach needs to be clearly articulated through informed debate that recognises that

21. Roth, Greenburg and Wille, 'Monograph on Terrorist Financing', p. 66.
22. Joyner, 'The United Nations and Terrorism', p. 252.
23. Roth, Greenburg and Wille, 'Monograph on Terrorist Financing', p. 64.
24. *Ibid.*, p. 63.
25. *Ibid.*
26. *Ibid.*
27. Darren W Davis and Brian D Silver, 'Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America', *American Journal of Political Science* (Vol. 48, No. 1, January 2004), p. 28.

'trade-offs between privacy and intrusion … reflect the different historical and social contexts in which they were made'.[28]

Critically, since the work of the 9/11 Commission, the data-analysis capabilities of banks and other financial institutions have advanced immeasurably; and whilst this perhaps provides grounds for further concern amongst those who believe that government restrictions on access to information are being rolled back ever further, the next section reveals that it also allows banks to be more targeted in their monitoring, reducing the risk of 'false positives'.

The Financial-Services View

Over the past twelve months, many banks and other financial institutions such as remittance companies have closely studied their exposures to Turkey and other states surrounding conflict-afflicted Syria. Given the size of the Turkish population and economy, and the resulting business potential for both corporate and consumer banking, international banks have spent the past 10–15 years investing heavily in efforts to gain a foothold in what should be a highly attractive market. The interaction banks have with Turkey ranges from buying stakes in local banks that offer full retail and corporate services to providing branch banking and advisory services to international corporate clients seeking to do business in Turkey. Most banks have some exposure to Turkey – exposure which to date has seemed like a wise investment decision but, during the past twelve months, has increasingly looked like a political liability.

The extent to which banks and financial institutions have sought to tackle this issue varies considerably. Some appear to have done little whilst most institutions interviewed for this study have undertaken a range of reviews. For example, some have studied the use of financial and banking services by their account and card holders of ATMs and credit-card terminals and have conducted extensive 'link analysis' of user activity. Others have reviewed their exposure to and the activity of clients operating in businesses associated with Daesh funding, particularly oil. Still others have scrutinised relationships with money-service businesses and NGOs closely. The analysis is not straightforward. Turkey's economy is well connected to international markets, making corporate financial transactions a common occurrence. Moreover, for those dealing with retail banking, the flood of tourists who visit Turkey's sites and beach resorts each year means that identifying the use of financial services by aspiring FTFs is highly challenging. Transaction monitoring can capture certain types of financial activity and deviations from traditional account-holder patterns but the vast majority of cases are false positives. Yet valuable information can be gathered which, when combined with other sources, can provide illuminating intelligence on account-holder or user activity.

28. Drozdova, 'Civil Liberties and Cyber Space', p. 9.

All financial institutions with connections to Turkey appreciate that heightened risks require enhanced awareness and due diligence, but implementing this additional security on anything but a 'best-guess' basis is challenging without some form of intelligence-based guidance from governmental authorities.

Box 4: Technology and Information Sharing in Practice.

As the authorities and the private sector grapple with ways in which information can be shared whilst addressing understandable privacy concerns, the following two projects are worth reviewing.

Ma³tch: A Model for the Future?

One possible model for the future of effective and secure information sharing that addresses privacy concerns has been developed by FIU.net, 'a decentralised computer network supporting the FIUs in the European Union in their fight against Money Laundering and Terrorist Financing'.[1] Ma³tch (known as 'Match 3') stands for 'Autonomous Anonymous Analysis',[2] and allows FIUs to compare data in an anonymised format according to the principle of 'privacy by design'.[3] Put simply, it converts data into 'uniform anonymised filters', which exclude sensitive personal information but allow FIUs to query the system in order to see whether other users have also registered the same subject, without revealing names and thus breaching privacy. If matches are returned, the FIU can then make a formal cross-border request for information related to their subject of interest. In this manner, FIUs can meet their responsibility to tackle money laundering and terrorist financing whilst at the same time protecting the privacy and personal data of EU citizens.

SWIFT and the Terrorist Finance Tracking Program

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) network is used by the majority of international banks to send interbank

1. For more details, see the FIU.net website at <www.fiu.net>.
2. For more details, see FIU.net, 'Ma³tch', <https://www.fiu.net/fiunet-unlimited/match/match3>, accessed 16 June 2015.
3. 'Privacy by design' refers to the inclusion from the outset of privacy measures in databases that 'avoid making costly mistakes later on, requiring expensive retrofits'. The design approach seeks to include key data-protection requirements such as data minimisation, privacy by default, data security and transparency. For more information, see Ann Cavoukian, 'Privacy by Design', Information and Privacy Commissioner of Ontario, 2009, <http://www.ipc.on.ca/images/Resources/privacybydesign.pdf>, accessed 16 June 2015; Paolo Balboni and Milda Macenaite, 'Privacy by Design and Anonymisation Techniques in Action: Case Study of Ma³tch Technology', *Computer Law and Security Review* (Vol. 29, No. 4, August 2013), pp. 330–40.

messages. The SWIFT network operates a standardised messaging system that allows banks to communicate internationally, issuing and receiving payment instructions. It provides the communication mechanism via which banks inform each other of the debits and credits they are making on behalf of one another – it does not transfer money, per se, a popular misconception. Daily traffic passing through SWIFT can reach over 25 million messages;[4] thus, given the extent of information flowing through SWIFT each day, it was not surprising when, in June 2006, it emerged that the US authorities were using subpoenas to access SWIFT transaction information as part of the US Treasury's Terrorist Finance Tracking Program (TFTP).[5]

The TFTP, created in 2001, 'enables the United States to examine financial transactions that rely on the messaging infrastructure provided by the Society for Worldwide Interbank Financial Telecommunications (SWIFT) for their completion'.[6] This programme was initially only open to use by the US, but in August 2010 the EU–US TFTP Agreement came into force, allowing the transfer and processing of data for TFTP purposes between the US and EU member states.[7] Under the EU–US agreement, the EU and its member states are allowed to use the TFTP for their own counter-terrorism investigations through reciprocity clauses.[8] A November 2013 report by the European Commission on the subject concluded that 'TFTP Provided Data, including data retained for multiple years, have been delivering very important value for the counter terrorism efforts in the United States, Europe, and elsewhere'.[9] This

4. SWIFT, 'SWIFT FIN Traffic', <http://www.swift.com/about_swift/company_information/fin_traffic_new>, accessed 16 June 2015.
5. Eric Lichtblau and James Risen, 'Bank Data is Sifted by U.S. in Secret to Block Terror', *New York Times*, 23 June 2006.
6. Justin Santolli, 'The Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive', *George Washington International Law Review* (Vol. 40, No. 2, 2008), p. 553.
7. US Treasury Department, 'Terrorist Finance Tracking Program: Questions and Answers', p. 1, <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/tftp_brochure_05062014.pdf>, accessed 16 June 2015; European Commission Migration and Home Affairs, 'Terrorist Finance Tracking Programme', <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/tftp/index_en.htm>, accessed 16 June 2015.
8. European Commission, 'Annex: Joint Report from the Commission and the U.S. Treasury Department Regarding the Value of TFTP Provided Data Pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program', COM(2013) 843 final, 27 November 2013, p. 9.
9. *Ibid.*, p. 2. See, for example, European Commission, 'Joint Review Report of the Implementation of the Agreement between the European Union and

report served only to support claims made at the time of the TFTP agreement by members of the George W Bush administration, who called the TFTP 'a vital tool' in the War on Terror,[10] and the US Treasury, which has claimed that the TFTP is 'exactly the kind of program that Americans want and expect from their government to prevent further terrorist attacks'.[11]

How TFTP Works

Through the TFTP, the US Treasury Department can access financial data that includes the amount transferred, bank account numbers, method of transfer, names of the parties involved, their addresses and telephone numbers, and information about the financial institutions involved in a transaction.[12] TFTP can therefore provide counter-terrorism officials with crucial pieces of information, such as locations, financial transactions and associates. Uses of data obtained via TFTP include identifying new streams of financial support and previously unknown associates, linking front entities and aliases with terrorist organisations, evaluating existing intelligence, and providing information that can be used to identify new targets.[13]

TFTP Safeguards

Given the extensive amount of information that is available through the TFTP, there has been significant scrutiny of the way in which it is used and the safeguards that are applied to avoid abuse of the programme. The TFTP's safeguards have been described by the US Treasury as 'rigorous'. Data can only be searched for counter-terrorism purposes, and no search can be conducted unless a TFTP investigator demonstrates a pre-existing nexus between the search's subject and terrorism or terrorism financing. The programme cannot be used for data mining or any other algorithmic profiling. Furthermore, independent overseers can block searches if they do not feel that all safeguards have been satisfied.[14]

---

the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program', SWD(2014) 264 final, 11 August 2014, pp. 41–43.

10. Patrick M Connorton, 'Tracking Terrorist Financing through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide', *Fordham Law Review* (Vol. 76, No. 1, 2007), p. 290.
11. US Treasury, 'Terrorist Finance Tracking Program', fact sheet, 2 August 2010, p. 2, <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/TFTP%20Fact%20Sheet%20revised%20-%20(8-8-11).pdf>, accessed 16 June 2015.
12. Santolli, 'The Terrorist Finance Tracking Program', p. 553.
13. European Commission, 'Annex: Joint Report from the Commission and the U.S. Treasury Department Regarding the Value of TFTP', pp. 5–6.
14. US Treasury Department, 'Terrorist Finance Tracking Program: Questions and Answers', pp. 2–4.

Under the EU–US TFTP Agreement, EUROPOL assesses 'whether the data requested in any given case are necessary for the fight against terrorism and its financing', and also verifies that requests are as narrow as possible as to minimise the amount of data requested.[15] In 2009, the European Commission declared that the US Treasury had 'from the outset, respected the safeguards in the handling of personal data obtained from SWIFT'.[16] The US Treasury also claims that 'regular, independent audits of the programme have confirmed that the US Government has consistently observed the established safeguards and protocols'.[17]

15. European Commission Migration and Home Affairs, 'Terrorist Finance Tracking Programme'.
16. SWIFT, 'Subpoenaed SWIFT Message Data is Adequately Protected', 18 February 2009, <http://www.swift.com/about_swift/shownews?param_dcr=news.data/en/swift_com/archived_news/press_releases_archive_subpoenaed_swiftmessagedata_adequatelyprotected.xml>, accessed 16 June 2015.
17. US Treasury, 'Terrorist Finance Tracking Program', p. 2.

The FIU View

In the English translation of its 2013 annual report, French FIU Tracfin provides great insight into the value it places on FININT, stating that: 'For the combating of terrorist financing, the detection of high-risk profiles by using financial intelligence is a very discrete way of adding to the information collected by the field units responsible for identifying and combating radical movements'.[29] Tracfin further notes that 'the investigators have access to multiple financial sources and a relatively broad scope of information', pointing in particular to the ability of banking information to produce a 'financial composite sketch of individuals suspected of belonging to a terrorist organisation'.[30] Tracfin even provides a case study (repeated in full in Box 5) of an individual who travels to a combat zone.

The overt focus of Tracfin on this issue appears unusual amongst its peers. Some FIUs and other government agencies have engaged with banks on, for example, analyses of the usage of ATM networks in key, related locations. As noted earlier in this chapter, the Australian FIU AUSTRAC provides clear transaction monitoring-related guidance in its recent review of terrorism financing in Australia, encouraging financial institutions to remain alert to the terrorist financing-related implications of political developments. However, beyond these piecemeal, national efforts, there is very little evidence that any meaningful form of systematic and strategic international effort exists to harness and empower the capabilities of the financial-services industry.

29. Tracfin, 'Annual Analysis and Activity Report 2013', p. 28, <http://www.economie.gouv.fr/files/ra_tracfin_anglais_2013.pdf>, accessed 16 June 2015.
30. *Ibid.*

Box 5: Case Study from French FIU Tracfin – an Individual Goes to a Combat Zone.

In terms of financial behaviour, there may be many warning signs indicating that an individual has decided to take action by leaving the country for a combat zone abroad.

For example, an individual's main objective may be to raise a maximum amount of funds in a short time. Initially, the rapid collection of funds is a core element of his activity. To achieve his or her goal, the individual applies for credit to several consumer loan institutions using false documents (pay slips, certificate from his employer and so on). These organisations are in fact able to provide funds very quickly, providing that the amount requested does not exceed a few thousand euros. During this preparatory phase, operating on these same principles, the applicant may also purchase a vehicle on credit. Shortly before his or her departure, once the funds have been paid by the credit organisations, the money is completely withdrawn in cash in one or more instalments. The account is rarely closed but its balance is close to zero and there are no further transactions. During this last stage of their preparations, the individual will also acquire the equipment they need, such as trekking equipment from a specialty shop. After the person has left the country, it is sometimes possible to follow his or her itinerary through expenses paid for by bank card and once he or she has reached the final destination, they can be followed through cash transfers sent to them by their support network such as family, friends and accomplices. In this last phase, it is particularly important for the FIU to have already identified as many targets as possible in the suspect's entourage, so as to detect any sources of financial support.

The FATF View

The global AML/CTF standard-setter, the FATF, recently produced a report considering the funding requirements and associated terrorist-financing risk of Daesh.[31] In it, the FATF noted the historic importance to Al-Qa'ida and affiliated groups of payments to fighters and the establishment of international recruitment hubs. It is perhaps the first document published by an international body that provides specific focus on financial issues related to FTFs, including case studies of financial activity that use known mechanisms such as bank transfers and money remitters and is thus open to monitoring and disruption. A number of cases and typologies are provided which suggest that collaboration between the authorities and financial-services industry could be invaluable.

31. FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)', February 2015, p. 36, <http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf>, accessed 16 June 2015.

The examples below are extracted from the FATF's report:[32]

- Finland has reported that a common methodology for financing FTFs is to send money via money remitters which have agents operating in border areas close to Daesh-held territory. This is to finance them once they are in Syria or Iraq
- The Netherlands authorities have observed that in some cases FTFs have to pay for their own living expenses and, to that end, receive funds from their respective home countries. Such transfers have been found to vary from several hundred euros to several thousand euros per transaction. The Netherlands has detected funds being transferred via regulated money and value-transfer systems to agencies located near territories where Daesh operates. Netherlands authorities regard it as highly likely that in other cases intermediaries transport cash to areas near territory occupied by Daesh. The Netherlands has also found indications that FTFs use debit cards that are linked to their national bank accounts when withdrawing money from ATMs close to those areas where Daesh operates
- Many FTFs also maintain access to their bank accounts. According to sensitive financial information provided by the US, terrorist-financing risk indicators were identified such as foreign cash withdrawals by unknown individuals from ATMs in areas located near territory where Daesh operates. Another terrorist-financing risk indicator identified was the depositing of large amounts of money into bank accounts that were immediately withdrawn, again in areas close to Daesh's activities. This information reveals the terrorism-financing risks posed by the continued ability of individuals – who are believed to have travelled to areas occupied by Daesh – to reach their bank accounts in their home countries.

Perhaps most importantly, the FATF acknowledges that more work needs to be done 'to develop red-flags to better identify the funding mechanisms FTFs utilize' and calls for 'greater domestic cooperation among AML/CFT bodies and other authorities'.[33] Including financial institutions in that work and ensuring that forward-looking advice is developed is clearly critical to the success and maximisation of these efforts.

The View from Turkey

As part of the research for this paper, interviews were conducted by Skype and telephone with individuals currently living in southern Turkey close to the Syrian border, most of whom have been displaced from Syria and are primarily working to send funds home to family members still inside the

32. *Ibid*., pp. 20–23.
33. *Ibid*., p. 36.

country. Whilst the information gathered from these conversations is far from exhaustive, a consistent picture appears with regard to financial flows. Considerable financial value flows to and from the border region, passing sometimes through local banks, but most often through informal money-transfer businesses. Jewellery and gold shops, often holders of significant cash floats, appear to be central to many of these flows.

Money-transfer businesses, often referred to as *Hawala* or '*Hawala*-like'[34] – reflecting the trust-based nature of the transfers and settlements – work best when there is a similar flow of funds between regions. Whilst the timing of transfers may differ, the fact that funds flow in both directions means that payments and receipts can be netted against each other, limiting the need for balancing payments to be made.

The Turkish border region provides a textbook example of this equilibrium.[35] Funds are transferred from Turkey into Syria by individuals who have crossed from Syria into Turkey to find work and who are remitting funds to family members left behind. In other cases, funds sent by donors in third countries such as the Gulf States are routed to Syria via money-service businesses in southern Turkey or Istanbul. These funds are sent in support of family members who have joined rebel groups or to support humanitarian aid efforts inside Syria. Funds coming in the reverse direction, from Syria into Turkey, are often sent to cover payment for supplies or are sent by those hoping to escape Syria for a new life somewhere in Europe and, fearing being robbed by those who smuggle them across the border, send funds ahead for collection on arrival. The amounts can be significant, running into the hundreds of thousands of dollars, as these transfers are often the result of the sale of land or property and represent an individual's life savings.

Whilst these flows of funds are almost impossible for the security authorities to monitor within the border regions, the remittance flow often extends beyond Gaziantep or Urfa, inbound from the Gulf or outbound via Istanbul to Germany, Greece or other destinations to which Syrian refugees are fleeing. These flows can also include funds transferred into the region by aspiring FTFs who, warned against carrying noteworthy sums of money as they travel

34. Such money-transfer businesses operate on a trust basis where the sending agent (in one location) requests that the receiving agent (in another location) pays out an agreed sum to the recipient without actually receiving funds. The sending agent will either balance its books via a physical cash transfer to the receiving agent at a later date to settle its debt or the receiving agent will request the sending agent to pay out to a recipient in its location, offsetting the initial payout that has been made. For the security and regulatory authorities, such forms of money transfer present significant challenges as whilst they are highly efficient and cost effective for users, they leave no meaningful 'financial footprints' for the authorities to follow.
35. As explained to the author during one Skype-based interview with an individual who facilitates the transactions referred to in this section.

to the border region, use informal mechanisms to send money ahead of their arrival. The FATF's recent report about Daesh's financing highlights cases of both remittance companies and NGOs being used to move money across Europe to Turkey in support of FTFs. Other examples of financial transactions revealed during interviews that might alert authorities to activity consistent with that of FTFs include the use of prepaid cards (a safer means of carrying financial value than bundles of cash) and consecutive daily-limit withdrawals from ATMs in southern Turkey.

Challenging though it may be, monitoring the flow of funds between Turkey and Syria on the one hand and Europe and the Middle East on the other can clearly provide invaluable insights into, and intelligence regarding, the activities of FTFs. Harnessing the capabilities of the financial-services industry in meeting this challenge is critical as whilst these funds do not always use the formal financial system, the amounts of money involved and the relatively advanced nature of the Turkish banking system mean that financial footprints are bound, at some point, to create a trail that can be used to illuminate the wider network of financial activity.

Piecing Together the Financial Mosaic

Alongside the initiatives being piloted in the UK by the Financial Sector Forum and the JMLIT, the security concerns raised by the rapidly evolving foreign-fighter phenomenon – in particular, the fear of 'blowback' impact on the fighters' home state should they return – is encouraging other FIUs to explore the value of information sharing with the financial-services industry. For example, some FIUs have worked with their local banks to review account-holder ATM activity in key locations. Others have undertaken an analysis of sources and uses of funds in an attempt to provide banks with FTF-specific red-flag indicators. Others still have encouraged banks to track the social-media activity of their account holders.[36]

Whilst the identified activities are certainly not individually suspicious, in combination they may create a picture worthy of further investigation. On their own, the purchase of airline tickets and camping or outdoor gear, and the withdrawal of an unusually large amount of cash from a bank account are hardly grounds for suspicion, given the activity is consistent with that of any avid outdoor traveller. However, when combined with account activity that indicates the holder is a receiver of meaningful state benefit payments; has made significant and unusual use of an overdraft limit; has taken a consumer loan that is in arrears or in default; has received an unusual number of typically small payments that might be from supporters or donors; has received a student loan but is not attending classes; or has closed an account

36. Chris Plecash, 'FINTRAC Looks to Banks to Monitor Clients' Social Media Activities', *Embassy News*, 25 February 2015.

via the withdrawal of cash rather than electronic transfer to a new account, a different picture begins to emerge.

Of course, identifying these characteristics through the standard transaction monitoring undertaken by financial institutions is highly challenging and will certainly produce a great many 'false positives' which must not be allowed to impact entirely innocent activity. It is precisely to help financial institutions separate the 'wheat' from the 'chaff' that a close and collaborative working partnership is needed between the public and private sectors, combining information from different sources such as passenger-name records or social-media activity, to determine whether the activity identified by a financial institution is indeed indicative of foreign-fighter or other terrorist activity.

Although relations between financial institutions and the security authorities appear to operate well when specific 'post-event' cases are being investigated, dialogue between banks and the authorities 'in the normal course of business' remains dysfunctional. Understanding of the needs and capabilities of each side is lacking. Interviews suggest that bankers do not find it helpful to be tainted with classified information but rather they want help in identifying macro themes, typologies and threats. Clarifying such misconceptions and developing a practical and productive modus operandi should be an urgent priority.

Furthermore, just as information sharing and partnership between the public and private sectors must improve, so too should the ability and willingness of different national and international agencies. Initiatives such as FIU.net's Ma^{3}tch provide an encouraging example of how privacy and security concerns can be reconciled.

Finally, banks themselves need to have greater freedom to share information related to money laundering and terrorist financing within their own organisations. As highlighted by Paul Saltzman, president of the US-based Clearing House Association, 'It is crucial that each bank have the ability to share suspicious activity reports and other AML-related information across its global organization to strengthen its ability to detect and prevent financial crimes'.[37] Clearly, if a bank is unable to communicate *within* its own organisation, its ability to contribute most effectively to AML/CTF efforts will be significantly hampered.

37. Clearing House, 'The Clearing House Provides Recommendations to FinCEN Aimed at Improving AML Compliance and Deterring Financial Crimes', press release, 16 March 2015, <https://www.theclearinghouse.org/press-room/in-the-news/2015/2015/03/20150316-press-release-on-sar-reports>, accessed 16 June 2015.

Box 6: A Working Model?

The partnership between financial institutions and the security authorities can perhaps be informed by developments elsewhere. As this paper has already noted, the UN has called on the airline industry to contribute to the work that the authorities are undertaking to combat terrorism in general and the flow of foreign fighters in particular. This model appears to work. For example, in August 2014, a sixteen-year-old girl was arrested at Nice airport as she attempted to fly to Turkey following a tip-off from Turkish Airlines to the French authorities. Suspicions were raised when the girl bought the ticket in cash and offered an unconvincing explanation of her reason for travel.[1]

1. John Lichfield, 'Suspected 16-Year-Old Wannabe Jihadist Arrested en route to Syria', *Independent*, 1 September 2014.

Conclusions and Recommendations

Unpalatable as it may be to acknowledge at a time when data protection is a high-profile topic – especially in the wake of the Snowden revelations – the financial-services industry holds data that provide significant insight into the habits and movements of its account holders. Consider the way in which online retailers such as Amazon or loyalty-card schemes such as Tesco Clubcard can anticipate a customer's purchasing interests – and this represents only a portion of an individual's financial transacting.

To an ever-increasing extent since 9/11, banks and other 'designated non-financial businesses and professions'[1] have been required to guard the national and global financial borders and take responsibility for the actions of their clients, documenting the source and destination of funds transfers that they facilitate. Being found to have handled illicit finance can have significant consequences. Witness the considerable fines levied on the banking industry in recent years.[2]

The stream of European citizens travelling to Syria to fight for Daesh has clearly caught national security authorities off guard. Although the identification and disruption of travellers is beginning to occur more regularly, thousands have already made the journey and many hundreds have also now returned home where (in some cases), radicalised, they may pose a threat to national security. The apparent failure of the security and law-enforcement authorities to harness the significant capabilities of the banks and other financial institutions in the identification of those who are planning to travel to, already on their way to or have arrived in Syria is, on the face of it, a missed opportunity and a significant failure. Had this relationship been effectively harnessed, it is likely that the authorities would have had a much better and more timely insight into an issue that has rapidly become a key security concern for most European countries.

The legal and technological challenges of building an effective partnership between the authorities and the financial-services industry should not be underestimated, but little systematic attempt appears to have been made to take advantage of either the capabilities financial institutions could bring to bear in tackling this threat or the 'Privacy by Design' techniques that are being deployed to help organisations share information on an anonymised

1. This is a 'catch-all' term used by the FATF to refer not only to institutions that handle large sums of financing (both cash and valuable property), but also to professional sectors such as lawyers and accountants who facilitate the movement and oversight of such activity.
2. For example, see fines of US$8.9 billion paid by BNP Paribas, US$667 million and US$300 million paid by Standard Chartered, and US$1.9 billion paid by HSBC.

basis.[3] Financial intelligence has proven invaluable in assisting with post-event investigations. It also has significant, untapped potential to enhance the intelligence picture the authorities use to identify and disrupt individuals conducting terrorist-related activity. Yet this potential is, in general, neglected despite the pressures placed on the financial-services industry to implement counter-terror finance-compliance regimes.

By way of conclusion, this Occasional Paper offers four observations and recommendations that should be urgently addressed if national authorities are to make effective use of what remains a neglected but potentially valuable counter-terrorism tool.

First, the authorities must properly understand what nature of information and intelligence is of value to the banking community in identifying terrorist activity. The sharing of classified information is clearly problematic. Even if individuals in banks are cleared to receive such intelligence, the use and further sharing of this information is challenging within a bank. However, bankers, in general, do not want or need classified information. They require thematic rather than entity-level information that allows them to deploy algorithms and filters within their transaction monitoring that alerts them to cases that call for further investigation. It is a clichéd image, but the more that the authorities can reduce the size of the haystack of information through which banks are required to sift, the more likely banks are to provide high-quality information in return.

Secondly, national security and law-enforcement agencies need to develop processes for sharing specific threat data with banks. Establishing a co-ordinated and intelligent process of producing and disseminating timely and detailed guidance to banks is a critical link that has been absent for too long – although nascent steps are finally being taken. For example, in the UK, the JMLIT has been established which can be used by the authorities to alert bank members of the taskforce to details disclosed to them via SARs. The British Bankers' Association should soon launch its Financial Crime Alerts Service that aims to use real-time intelligence pooled from twelve partner agencies – including the NCA – to help banks tackle financial crime.[4] By disseminating intelligence in this manner, the authorities can ensure that relevant security information is shared across the banking community as well

3. For more detail on the issue of 'privacy by design', see Paolo Balboni and Milda Macenaite, 'Privacy by Design and Anonymisation Techniques in Action: Case Study of Ma[3]tch Technology', *Computer Law and Security Review* (Vol. 29, No. 4, August 2013), pp. 330–40.
4. British Bankers' Association, 'Banks Team up with Government to Combat Cyber Criminals and Fraudsters', 23 September 2014, <https://www.bba.org.uk/news/press-releases/banks-team-up-with-government-to-combat-cyber-criminals-and-fraudsters/#.VRgs347F-Sp>, accessed 16 June 2015.

as between individual banks and the authorities, thus ensuring information vacuums are avoided.

Thirdly, and closely related, barriers to information sharing within the public sector and within individual banks must be addressed. Systems such as Ma^{3}tch being developed by FIU.net could play a valuable role in facilitating the matching of cross-border FININT, while an urgent overhaul of the information-sharing regulatory framework for banks also needs to be undertaken. As things stand, on both counts, the restriction on information sharing significantly hampers efforts to tackle money laundering and terrorist financing.

Finally, the authorities need to produce forward-looking financial threat assessments. Too much guidance is provided on a historical basis. For example, recent reports from the FATF and other multilateral organisations such as the UN provide some useful insights into the past modus operandi of Daesh, but give no consideration to how this model might evolve. Financial institutions require this insight if they are to be able to contribute the valuable intelligence they may hold. Whereas financial institutions have a significant pool of experience on which to draw when tackling fraud and other forms of financial crime, they are less well equipped to identify activity consistent with FTFs unless supplied with typologies by those better informed, namely the security authorities.

The FTF phenomenon has caught security authorities across the globe off guard. Authorities in many Western capitals only awoke, belatedly, to the threat once many hundreds of their citizens had made the journey to Syria and had begun openly to promote their actions via social media. Significant resources are now being mobilised to combat the threat posed by returning radicalised jihadi fighters. For too long, banks have been held accountable for protecting the financial borders without being appropriately empowered to do so effectively. The threat posed by FTFs should provide urgent impetus for this weakness to be addressed, using the financial footprints left by FTFs to illuminate both their activity and that of the wider network to which they are connected. The financial sector has the capability to act as a significant 'force multiplier' for the security authorities.[5] Neglecting this capability is a security weakness that must be urgently addressed.

5. David Cohen, US under secretary for terrorism and financial intelligence, speaking at the Royal United Services Institute (RUSI), June 2014, London.

About the Author

Tom Keatinge is Director of the Centre for Financial Crime and Security Studies at RUSI. Prior to this, Tom had a twenty-year career at J.P. Morgan. In 2011–12 he took a sabbatical from J.P. Morgan to study for a Master's in Intelligence and International Security at King's College London where he wrote his dissertation on the operation and effectiveness of the global counter-terror finance regime. He now focuses his research on the field of 'finance and security', considering a number of themes including: the use of financial warfare to disrupt terrorist and insurgent groups; the use of FININT as a security tool; and enhancing security via public-private partnerships.

IDENTIFYING FOREIGN TERRORIST FIGHTERS

The Role of Public-Private Partnership, Information Sharing and Financial Intelligence

Tom Keatinge

Among today's most pressing global security threats is the risk created by individuals travelling to fight with groups in Syria and Iraq, where they may be radicalised. Of these many thousands, it is feared that some will return home, potentially with the intent of inflicting violence on those they view as enemies of Islam. Indeed, Daesh urges its supporters – via its *Dabiq* magazine – to target 'citizens of crusader nations … wherever they can be found'. These so-called 'foreign fighters' have flocked to Syria and Iraq in their thousands. Whilst the vast majority comes from Arab countries, a significant minority of as many as 4,000 comes from Western states, including most countries of the EU.

Since 9/11, financial institutions have found themselves placed squarely on the front line of efforts to combat terrorism as the global community seeks to undermine the financing of terrorism, targeting the perceived Achilles' heel of groups such as Al-Qa'ida, Al-Shabaab and Daesh. Banks have played valuable 'post-event' investigative roles such as following the London transport bombings in 2005, but could they play a role in disrupting future terrorist threats already in the planning? This Occasional Paper considers the role that banks, armed with troves of financial data, might play in revealing the financial footprints of those travelling to join jihadi groups in Syria and Iraq or having returned home.