Royal United Services Institute
for Defence and Security Studies

Occasional Paper

A Sharper Image

Advancing a Risk-Based Response to Terrorist Financing

Tom Keatinge and Florence Keen

A Sharper Image

Advancing a Risk-Based Response to Terrorist Financing

Tom Keatinge and Florence Keen

RUSI Occasional Paper, March 2020

Royal United Services Institute
for Defence and Security Studies

189 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 189 years.

Published in 2020 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, March 2020. ISSN 2397-0286 (Online); ISSN 2397-0278 (Print).

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

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Acknowledgements v

Executive Summary vii

Introduction **1**

I. Balancing a Dual-Purpose Regime **7**
- Depriving Terrorists of Funds 7
- Using Financial Intelligence to Detect and Disrupt Terrorist Networks 9
- CTF and Public–Private Partnerships 11
- Recommendations 13

II. Risk Profile **17**
- Territory-Controlling Groups 19
- Fundraising Methods 21
- Movement of Funds 25
- Storage and Investment 28
- CTF Responses 29
- OCG-Type Groups 30
- Lone Actors and Small Cells 39
- Recommendations 46

III. New Technologies and Terrorism Finance **51**
- FinTech 51
- Social Media 54
- Recommendations 56

IV. Sharpening the Response **59**
- FATF's Shift Towards Effectiveness 59
- Taking Ownership 67
- Recommendations 68

Conclusion **71**

About the Authors 73

Acknowledgements

Over the lifetime of this project, a considerable number of people have kindly and willingly provided us with their time and expertise. We are grateful to the wide range of experts from governments, multilateral organisations and the private sector who agreed to be interviewed by us, provided us with opportunities to present our work and contributed valuable feedback on our findings as they developed. We are particularly grateful to the members of the project advisory board who took the time to travel to RUSI to guide our process and contribute to our deliberations. Particular thanks are also due to RUSI Research Fellow Anton Moiseienko and RUSI Associate Fellow David Artingstall who contributed valuable research and writing input to this paper as well as forensic feedback on an early draft.

Thanks are also due to the RUSI Publications team who, as ever, dealt with the vagaries of researchers' time-keeping; as well as our peer reviewers, Katherine Bauer, Jimmy Gurulé and Inês Sofia Oliveira, who kindly accepted the 30,000-word challenge.

And finally, many thanks to PMI Impact, a global funding initiative by Philip Morris International, that provided the financial support necessary to run this project over the past two-and-a-half years. Their willingness to be flexible as our timetable developed and we adapted to circumstances has been very much appreciated and allowed us – we hope – to make the best use of their generous funding.

Executive Summary

SINCE 9/11, TARGETING the finances of terrorist actors has been a central element of the global counterterrorism landscape, commonly known today as the counterterrorist financing (CTF) regime. Indeed, the first shot fired by George W Bush in his 'War on Terror' was a financial measure in the form of Executive Order 13224, announcing a strike on 'the financial foundation of the global terror network' intended to 'starve the terrorists of funding'.[1]

Yet nearly 20 years on, that clearly defined objective remains elusive. In that period, the Islamic State expanded to control vast swathes of Iraq and Syria, sourcing funding from the territory it controlled. Groups such as Hizbullah have grown to operate lucrative transnational business operations, and small-cell and lone-actor terrorism, which is often low- or no-cost, has wreaked havoc in Western and other cities. The 'global terror network' and its 'financial foundation' has turned out to be a patchwork of multiple networks of various actors – including emerging or resurging threats such as the extreme right wing – and diverse funding methods.

The CTF regime, as conceived after 9/11, was structured with the specific risk posed by Al-Qa'ida in mind. Assessments of CTF effectiveness review the progress made since 9/11 in implementing the architecture called for by the UN and other leading bodies such as the Financial Action Task Force (FATF), based on this post-9/11 model. The foundational elements of that model, including the criminalisation of terrorist financing, remain relevant. Other aspects, such as the focus on wire transfers and charities, while still relevant against certain risks today, reflect the specifics of the terror finance threat landscape at the time. However, that landscape has evolved, and so too should the global response.

Not only has the threat picture changed, but so has the global environment within which terror funding takes place. Globalisation, new technologies and new payment systems are vulnerable to terror funding as much as they are to exploitation by serious and organised crime groups. A balance must be struck in promoting the societal benefits such innovations can bring and the new risks they facilitate.

There have also been significant developments in cooperation and information sharing on financial crime generally, between investigative and intelligence agencies and with the private sector, sometimes modelled on informal arrangements that came about to tackle specific terrorist risks. Counterterrorism efforts are often rooted in security services or specialist police agencies, which may still have more to learn about the benefits that financial intelligence can bring to their operations. Extending public–private information sharing to include these

1. US Treasury Department, 'Contributions by the Department of the Treasury to the Financial War on Terrorism: Fact Sheet', September 2002, p. 2.

agencies, or information originating with them, and financial technology and other sectors is a challenge, but one that must be addressed.

The 20th anniversary of the adoption of the text of the UN's International Convention for the Suppression of the Financing of Terrorism (the CTF Convention)[2] offers an opportunity to consider whether the global and national response to terrorist financing is addressing the challenges that it – and the many subsequent UN Security Council Resolutions, FATF Recommendations, guidance papers and high-level political communiqués – set out to tackle. It also provides an opportunity to assess whether the approach taken to identifying and disrupting terrorist financing needs to undergo a step-change again, just as it did after 9/11.

Over the past two years, through a grant provided by PMI Impact,[3] the authors have had the opportunity to consider these issues in a wide-reaching study of CTF literature and policy documents, in addition to interviews with experts and practitioners across four continents.

The project findings reveal that, on the whole, the global response to terrorist financing remains one-dimensional, despite the multi-faceted risk picture. Although initially conceived as a distinct and dedicated response to the 9/11 attacks, countries most often treat terrorist financing as an adjunct to money laundering.[4] As this paper will discuss, central to developing a more effective response to terrorist financing is recognising the variety of ways in which terrorist actors raise funds. Whereas a response based on anti-money laundering may be relevant in some cases, this is far from always being so.

Furthermore, in many countries, the response to terrorist financing remains predicated on a threat and funding model that has not evolved since 9/11 and thus fails to consider the risks posed by other forms of terrorist actor, including: territory-controlling groups; organised crime-type groups; and lone actors and small cells inspired (if not directed by) larger terrorist groups abroad. It is time to develop a more nuanced and risk-specific response to terrorist financing that is not merely rooted in the post-9/11 response to Al-Qa'ida.

Since 9/11, the risk landscape – and the means by which terrorist actors fund themselves – has evolved, yet the global response has been slow to react, diminishing its effectiveness. For much of the period since 9/11, policymakers and national leaders have placed an unequal emphasis on cutting off funds within the formal financial system. One academic noted that this narrative was 'over-hyped' in the wake of 9/11, and thus promised more than it could achieve.[5] Tackling a terrorist group's finances is far more challenging than simply switching off a tap. Groups adapt

2. UN General Assembly, 'International Convention for the Suppression of the Financing of Terrorism', adopted by Resolution 54/109, 9 December 1999, No. 38349.
3. For further information, see PMI Impact, 'Report 2019: Combating Illegal Trade, Together', 2019.
4. Tracey Durner and Danielle Cotter, 'Untangling a Marriage of Convenience Anti-Money Laundering and Countering the Financing of Terrorism', The Global Center on Cooperative Security, January 2019.
5. Authors' interview with UK-based academic, London, March 2019.

their strategies to respond to financial pressure; lone actors and small cells operate with little or no funding and that which they do use is often from legitimate sources such as salaries or benefits. Money will always find a way to flow, and disrupting this flow is an important objective, but should never be the sole pillar on which the response to terrorist financing is built.

This Occasional Paper is targeted at policymakers, law enforcement agencies and private sector actors that are tasked with combating terrorist financing. It provides an assessment of the different forms of terrorist actor and proposes ways in which a more informed and dynamic response to terrorist financing could be developed, with the following principles in mind.

Clarify the Objectives of CTF Measures

- Much of the research for this paper suggests that the specific objective of the global CTF regime has become confused. Thus, it is critical to ensure that CTF measures are risk-based and focus on achievable objectives, including the identification and disruption of:
    - The resourcing of terrorist organisations.
    - The financing of specific terrorist acts.
    - Terrorist activity, by using financial intelligence proactively and reactively.
- Promote better public and expert awareness of CTF objectives so as to minimise unjustified scepticism (for instance, the argument that CTF measures are ineffective because terrorist attacks still happen).

Develop Evidence-Based CTF Strategies

- Conduct terrorist financing-dedicated national and regional risk assessments via regional FATF bodies and tailored risk assessments.
- Assess countries for terrorist financing transit risk, as well as source and destination risk.
- Ensure responsible discussion of evidence; avoid inflating terrorist-financing risks such as the alleged role of wildlife trade finance for Al-Shabaab in Somalia.
- Apply greater scrutiny to terrorist actor forms and funding methods to devise targeted CTF responses.
- Identify specific vulnerabilities to target. For example, improve understanding of how groups move funds internationally.
- Identify and engage key terrorist resource suppliers (such as van hire companies or chemical retailers) to respond to the rise of low-/no-cost terrorism that does not rely on fundraising.
- Study the experience of tackling similar terrorist and related financing risks across geographies and time.
- Adapt CTF responses to developing threats including extreme right-wing terrorism that may employ novel financing methods (for example, raising funds via music festivals).
- Promote greater private sector awareness of, and engagement in, evidence gathering and activity identification.

Make Greater Use of Financial Intelligence

- Recognise that CTF measures should focus not only on depriving terrorists of funds, but also on using financial intelligence against their operations to the best effect.
- The use of financial intelligence should be integrated with more commonly exploited intelligence sources and used to support non-financial aspects of a terrorism investigation.

Promote Collaboration

- Between counterterrorism and law enforcement officials:
  - Target professional enablers providing 'crime as a service'.
  - Ensure links between crime and terrorist activity are investigated and exploited.
  - Implement Hague Good Practices on addressing the nexus between transnational organised crime and terrorism.
- Between public and private sectors:
  - Consider models such as the UK Joint Money Laundering Intelligence Taskforce's Terrorist Financing Expert Working Group, and the Netherlands Terrorist Financing Taskforce.
- Between countries and within regions:
  - Consider models such as: the Southeast Asia CTF Summit; the Europol Financial Intelligence Public Private Partnership; and the US-led Law Enforcement Co-ordination Group, an international effort to raise awareness of and increase coordination against Iran and Hizbullah's broad range of terrorist and criminal activities around the world[6] and the recently launched Counter-Hizballah International Partnership (CHIP).[7]
  - Develop and promote country- and region-specific terrorist financing typologies.

Engage More Actively with Risks Posed by New Technologies

- Ensure understanding of terrorist use of cryptocurrencies remains current and drive internationally consistent standards of crypto-industry supervision.
- Develop more active CTF engagement with new payment platforms and include financial technology companies in public–private information sharing partnerships.
- Dedicate resources to training financial investigators, prosecutors and judges in understanding the abuse of financial technologies.
- Drive greater focus on terrorist financing by social media companies; ensure terms of service and community standards explicitly reference and prohibit terrorist financing, and that social media companies intervene against abuse and misuse accordingly to restrict the use of their platforms for promoting calls for terrorist financing.

---

6. Matthew Levitt, 'America May Have Unlocked a Key to Fighting Terrorism – And it Doesn't Involve Drones', *Washington Post*, 7 January 2016.
7. US Department of the Treasury, 'Treasury Launches the Counter-Hizballah International Partnership [CHIP] to Thwart Illicit Financial Activity', 18 October 2019.

- FATF should underpin this requirement for social media companies to strengthen their standards and governance by building on the work undertaken by two of its regional bodies[8] to prioritise raising awareness among its member states of the terrorist financing vulnerabilities posed by social media, including producing specific guidance.

8. Asia Pacific Group (APG)/Middle East North Africa (MENA) Financial Action Task Force (FATF) Report, 'Social Media and Terrorism Financing,' January 2019.

Introduction

ON 23 SEPTEMBER 2001, President George W Bush signed Executive Order 13224,[1] authorising the US government 'to designate and block the assets of foreign individuals and entities that commit, or pose a significant risk of committing, acts of terrorism'. The order also allows for the blocking of 'the assets of individuals and entities that provide support, services, or assistance to, or otherwise associate with, terrorists and terrorist organizations designated under the Order, as well as their subsidiaries, front organizations, agents, and associates'.[2]

The importance of this Order was revealed by evidence that Al-Qa'ida had spent between $400,000 and $500,000 to finance 9/11, much of which passed undetected through the formal financial system.[3] What followed was the emergence of the global counterterrorist financing (CTF) regime. A raft of terrorist financing-related UN Security Council Resolutions (UNSCRs) and the Financial Action Task Force's (FATF) 'Special Recommendations' were published, requiring countries to establish the required legal and operational CTF structures and heightening the emphasis placed on financial institutions, as the first line of defence, to detect and report suspicions of terrorist financing to law enforcement in their jurisdictions.

Immediately after 9/11, the logic for the creation of such a global and national CTF architecture was clear. Much of the funding required to support and launch the attacks had flowed through the formal banking system. It followed, therefore, that securing the financial system from abuse by terrorist actors would severely restrict their ambitions.[4]

At the time of 9/11, the idea that targeting terrorists' funding would restrict their activities was not new. On the international stage, the UN member states had adopted the International Convention for the Suppression of the Financing of Terrorism[5] (the CTF Convention) in 1999,

1. US Department of State, Executive Order 13224 (2001).
2. US State Department, Bureau of Counterterrorism and Countering Violent Extremism, 'Executive Order 13224 – Learn More'. In September 2019, President Donald Trump updated Executive Order 13224 'to consolidate and enhance sanctions to combat acts of terrorism and threats of terrorism'. See The White House, 'Executive Order on Modernizing Sanctions to Combat Terrorism', 10 September 2019.
3. John Roth, Douglas Greenburg and Serena Wille, 'National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing – Staff Report to the Commission', 2004, p. 3.
4. *Ibid.*
5. UN General Assembly, 'International Convention for the Suppression of the Financing of Terrorism', adopted by Resolution 54/109, 9 December 1999, No. 38349.

but only four countries[6] had ratified the Convention by September 2001. Countries such as the UK, which already had a history of dealing with political violence in Northern Ireland, had long viewed CTF as a pillar of its counterterrorism response.[7]

But despite localised initiatives, the idea that targeting terrorist financing should be pursued on a global basis had failed to catch on. 9/11 changed that dynamic.

Using its global diplomatic muscle – and harnessing the worldwide support it received following the attacks – the US drove a relentless effort to target terrorist financing as part of its broader effort to counter the risk posed by Al-Qa'ida. The focus on identifying and freezing terrorist assets was a central – and visible – element of this effort to restrict terrorist activity.[8] Domestically, the USA PATRIOT Act was passed, Title III of which introduced a range of measures, the purpose of which was 'to increase the strength of United States measures to prevent, detect, and prosecute international money laundering and the financing of terrorism'.[9] Internationally, the UN passed UNSCR 1373 that called on member states to take a range of measures to prevent and suppress the financing of terrorist acts;[10] and the FATF, the global anti-financial crime standard setter that had hitherto restricted its focus to money-laundering, had terrorist financing added to its mandate.[11]

Although this concept of a 'CTF' regime became commonplace following the advent of FATF's Special Recommendations, introduced after 9/11,[12] terrorist financing is by no means a modern-day concept. The 17th-century Italian General Raimondo Montecuccoli reportedly noted that three things were necessary to wage war – money, money and money.[13] This observation predates the emergence of the word 'terrorism', let alone its use in its modern sense.[14] Yet contemporary counterterrorism policies are also based, in part, on the premise that anyone using force over an extended period of time to achieve political objectives requires resourcing to succeed. As a corollary of these policies, the notion of turning an adversary's financial needs into a vulnerability has developed. In his 2002 paper, 'The Four Waves of Rebel Terror and

6. Botswana, Sri Lanka, the UK and Uzbekistan. See UN Treaty Collection, 'International Convention for the Suppression of the Financing of Terrorism', 9 December 1999.
7. Ed Moloney, *A Secret History of the IRA* (London: Norton Books, 2002).
8. For a detailed examination of this effort, see Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York, NY: PublicAffairs, 2015).
9. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.
10. UNSCR 1373, 28 September 2001, S/RES/1373.
11. FATF, 'FATF IX Special Recommendations', October 2001 (incorporating all subsequent amendments until February 2008).
12. *Ibid.*
13. N E Dreisziger, 'Montecuccoli, Raimondo, Prince', in Stanley Sandler (ed.), *Ground Warfare: An International Encyclopaedia,* Vol. 1 (Santa Barbara, CA: ABC Clio, 2002), p. 588.
14. Merriam-Webster, 'The History of the Word "Terrorism"'.

September 11',[15] David Rapoport provides a useful financial perspective. He first describes the revolutionary groups of the 1800s[16] that deliberately sought political targets to further their goals, financing their activities through bank robberies; followed by the formation of post-First World War groups that sought independence from British colonial rule, and whose financing tactics relied less on bank robberies, in part because diaspora sources supporting independence provided considerable funds.

Rapoport's paper then outlines the strategies of groups in the second half of the 20th century, including ETA and the Palestine Liberation Organisation, which engaged in kidnap for ransom, and Colombia's Revolutionary Armed Forces of Colombia (FARC), which profited widely from drug trafficking, demonstrating the capacity of terrorist organisations to behave in a similar way to transnational organised crime groups. The paper goes on to describe the emergence of religious terrorism in the 1970s, which was not limited to, but dominated by, Islamism – in particular, Sunniism – the climax of which was the emergence of Al-Qa'ida and the 9/11 attacks.

While Rapoport's conceptualisation would require updating to account for the further events of the 21st century, it is a useful description of the evolution of terrorists and their financial behaviour, and underlines the longevity of this issue. Groups engaged in asymmetric warfare have always required finances to achieve their objectives.

Almost two decades on from 9/11, the global response is still fundamentally based on the architecture that was put in place in the immediate aftermath of the attacks. The emergence of Islamic State (also known as ISIL/ISIS) in 2014 and its considerable fundraising aptitude[17] drove the issue of terrorist financing back to the top of the political and policy agendas. It is thus timely and appropriate to reassess this regime and what it can – and should – achieve, particularly given the dichotomy between the statements made by political leaders expressing their belief in the effectiveness of 'cutting off' terrorist financing,[18] and the view of some that 'the war on terrorist financing has failed'.[19] In practice, this is a false choice, suggesting a binary decision for those in the public and private sectors charged with combating terrorist financing, whereas a more nuanced and risk-based response is required.

15. David Rapoport, 'The Four Waves of Rebel Terror and September 11', *Anthropoetics* (Vol. 8, No. 1, Spring/Summer 2002).
16. For example, revolutionary groups that emerged across the Russian empire in the 1880s during the anarchist wave, such as the *Narodnaya Volya* ('The People's Will').
17. Tom Keatinge, 'Finances of Jihad: How Extremist Groups Raise Money,' *BBC News*, 12 December 2014.
18. *Associated Press*, 'More Than 70 Countries Commit to Combat Terrorist Financing', 26 April 2018.
19. Peter Neumann, 'Don't Follow the Money: The Problem with the War on Terrorist Financing', *Foreign Affairs*, July/August 2017. For a wide-ranging critique of the post-9/11 counterterrorism response, including on terrorist financing, see R T Naylor, *Satanic Purses: Money, Myth, and Misinformation in the War on Terror*, (Montreal: McGill-Queen's University Press, 2006).

Moreover, the rise, primarily in Western countries, of low- or no-cost terrorism, in which individuals and small cells manufacture attacks quickly, with often fatal results, challenges the notion of CTF as originally conceived given the evident difficulty of identifying such small amounts of money, much of which comes from legitimate sources.

During the lifetime of this project, there have been some welcome developments such as the passing in March 2019 of UN Security Council Resolution 2462 covering a range of issues previously unaddressed by the UN, underlining the need to move beyond an approach rooted in the post-9/11 response;[20] the establishment and growth of the regional Southeast Asian CTF Summit and accompanying collaborative infrastructure; and the CTF focus of the new financial crime public–private partnerships that have been developed in countries such as the UK or the Netherlands. But these are exceptions. Many jurisdictions have not adequately assessed terrorist-financing risk and thus their CTF policies are not informed by the appropriate risk assessment;[21] and political leaders still call for terrorist financing to be disrupted as if there is a tap that can be turned off to deprive terrorist actors of their funding.[22] In contrast, the role of financial intelligence remains under-emphasised and under-exploited, jurisdictions that have not suffered terrorist attacks often fail to query whether they might be part of the terrorist-financing supply chain nonetheless, and the guidelines, recommendations and requirements put forward by UNSCRs and FATF remain poorly implemented.

As the title of this paper suggests, the authors believe it is time to sharpen the approach to CTF. Against a backdrop of the evolving terrorism threat, varied terrorist financing modi operandi, and a more engaged financial sector, the authors argue that greater emphasis should be placed on the intelligence value that finance provides. This is required to develop a more nuanced and sophisticated framework for combating terrorist financing and using finance – and related intelligence – as a tool to fight terrorism, complementing the (often unrealistic) call for terrorist financing to be disrupted. As the 9/11 Commission Report proposed, government agencies should 'expect less from trying to dry up terrorist money and more from following the money for intelligence, as a tool to hunt terrorists, understand their networks, and disrupt their activities'.[23] Belatedly, this approach is beginning to gain greater recognition.[24]

20. UNSCR 2462, 28 March 2019, S/RES/2462.
21. Eastern and Southern African Anti-Money Laundering Group, 'Regional Counterterrorist Financing Operational Plan (2018/2020)', Pen.doc 6 (2018).
22. Theresa May, 'G20 Summit July 2017: Prime Minister's Press Statement', 8 July 2017; *Times of Israel*, 'Macron Calls for Global Cooperation to Cut Off Funds to Terrorists', 27 April 2018.
23. 9/11 Commission Report, 'Final Report of the National Commission on Terrorist Attacks Upon the United States', Executive Summary, July 2004, pp. 18–19.
24. See UNSCR 2462, operating paragraphs 19(b) and (c).

Objective

At the beginning of this project, the central hypothesis was that the CTF regime lacked clarity and purpose, meaning different things depending on any given actor's perspective – thus skewing assessments of success.

The focus that has been applied to terrorist financing by multilateral organisations appears to have engendered a 'top-down' response. As one interviewee noted, countries might take CTF action when centrally directed by a UN sanctions listing, but most do little individual risk assessment.[25] This becomes increasingly apparent as the varied nature of terrorist financing today is considered. The majority of the literature remains rooted in the post-9/11 introduction of the CTF regime and the response to Al-Qa'ida, with far less consideration given to the way in which certain threats have become more prominent or evolved and the CTF response has diverged as a result.[26]

With this background in mind, this paper seeks to provide an approach through which a more appropriate and relevant response to terrorist financing can be developed by individual countries, based on an understanding of risk and related finance, rather than the application of a generic 'top-down' framework that lacks informed focus.

Methodology

This project based its analysis on interviews with subject matter experts and publicly available literature on terrorism and terrorist financing. The literature review included publications by international organisations, domestic governments and law enforcement agencies, non-governmental agencies and academics. The literature review is integrated throughout the paper as the diverse nature of the material makes it more relevant when disaggregated. The project relied on semi-structured interviews as the most appropriate qualitative method of evidence gathering due to their flexible nature,[27] ensuring that major topics were covered while not limiting participants to predetermined ideas or theories.

---

25. Authors' interview with multilateral policymaker, New York, January 2019.
26. Michael Levi, 'Combating the Financing of Terrorism: A History and Assessment of the Control of Threat Finance', *British Journal of Criminology* (Vol. 50, No. 4, July 2010), pp. 650–69; Jonathan M Winer and Trifin J Roule, 'Fighting Terrorist Finance', *Survival* (Vol. 44, No. 3, 2002), pp. 87–104; Juan Miguel del Cid Gomez, 'A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates', *Perspectives on Terrorism* (Vol. 4, No. 4, October 2019), pp. 3–27; Thomas J Biersteker and Sue E Eckert (eds), *Countering the Financing of Terrorism* (London: Routledge, 2008); Arabinda Acharya, *Targeting Terrorist Financing: International Cooperation and New Regimes* (Abingdon: Routledge, 2009); Jae-myong Koh, *Suppressing Terrorist Financing and Money Laundering* (New York, NY: Springer, 2006); Nick Ridley, *Terrorist Financing: The Failure of Counter Measures* (Cheltenham: Elgar, 2012).
27. Eric Drever, *Using Semi-Structured Interviews in Small-Scale Research: A Teacher's Guide* (Glasgow: Scottish Council for Research in Education, 1995).

The project team conducted interviews (both by telephone and in person) with participants from Australia, Belgium, Canada, France, Germany, Indonesia, Israel, Italy, the Netherlands, the Philippines, Singapore, the Republic of Ireland, Russia, the UAE, the UK and the US. These included representatives of governments, law enforcement agencies, the private sector and academia. The interviewees were identified based on their professional activities, publication record or recommended by other interviewees. The interviews were conducted in an off-the-record capacity, ensuring the anonymity of interviewees, thus enabling them to be candid in their answers.

There were two objectives of the interviews: to obtain up-to-date information or perspectives on issues that were not sufficiently addressed in the existing literature; and, if applicable, to discuss current innovations and potential future improvements to counterterrorism or CTF efforts in the area of the interviewee's expertise. Interviews were planned with a view to speaking to a range of practitioners and policymakers in a variety of different regions, to ensure that the project findings would be applicable globally while reflecting the regional discrepancies inherent in terrorist financing and subsequent CTF policies.

The limitation of this method is that by using a selection of interviewees from a limited number of countries, there will be perspectives that have been missed. The authors sought to mitigate this by including a diverse range of participants, including those who challenged the status quo. Moreover, to ensure the accuracy and relevance of the project's findings and recommendations, provisional findings and recommendations were discussed at the meetings of the project's advisory board, which brought together 20 UK-based and overseas policymakers, law enforcement officers and academics. Advisory board meetings were convened three times throughout the project.

The paper has four chapters. Chapter I assesses the two fundamental principles of the global CTF regime: depriving terrorists of funds; and using financial intelligence to detect and disrupt terrorist networks. Chapter II outlines the profile of various forms of terrorist threat, distinguishing between three main types of terrorist actor: territory-controlling groups; organised crime (OCG)-type groups; and small cells and lone actors (whether directed, inspired or self-motivated), and argues for a CTF response tailored to the specific risk. Chapter III discusses new payment methods, new technologies and terrorism finance, including FinTech and social media, reflecting the expanding nature of terrorist-financing tools since 9/11 and the need for responses to consider such developments. Chapter IV considers the effectiveness and ways in which the global response to terrorist financing can be sharpened. Recommendations are provided at the end of each chapter with the overall project conclusions summarised in Chapter V at the end of the paper.

I. Balancing a Dual-Purpose Regime

WHEN CONSIDERING THE methods taken to combat terrorist financing by states, their law enforcement and intelligence agencies and private sectors, the authors posit that two overarching approaches should be followed: depriving terrorists of funds; and using financial intelligence to detect and disrupt terrorist networks.

The first, cutting off terrorist finance to prevent terrorist attacks, has become the most publicly championed element within the CTF architecture, frequently aired by global leaders and policymakers in the wake of terrorist attacks.[28] Calling for this kind of response to terrorist financing is appealing and the logic appears sound, but in reality cutting off a terrorist group's access to finance is more challenging than simply switching off a tap. Groups adapt their strategies to respond to financial pressure; lone actors and small cells operate with little or no funding and the funding they do use is often from legitimate sources such as salaries or benefits. Money will always find a way to flow – disrupting this flow is an important objective, but should not be the sole pillar on which the response to terrorist financing is built.

In contrast to the focus placed on identifying and severing financial connections, the use of financial intelligence to uncover networks and identify suspicious activity has been rarely promoted by the same political leaders. Likewise, with few notable exceptions, interviews for this paper found little engagement in law enforcement and policy circles with the opportunities afforded by financial intelligence. Yet financial intelligence can be a valuable asset, revealing connected individuals and their associates, communication methods and travel patterns. Therefore, developing a deeper understanding of, and applying stronger emphasis to, the use of financial intelligence should be prioritised. Cutting off terrorist funds or following the financial connections need not always be a binary choice. These objectives and their related tools should be complementary and prioritised according to circumstances, as this chapter will explore.

Depriving Terrorists of Funds

As noted above, much of the CTF rhetoric focuses on a particular form of terrorist threat and endeavours to deprive them of the revenue and/or other resources they need to operate

28. For example, in the wake of the November 2015 Paris attacks, France's chief prosecutor Francois Molins stated: 'We have to find out where they came from … and how they were financed'. See *BBC*, 'Paris Attacks: Prosecutor Molins Says Three Teams Involved', 15 November 2015. Theresa May stated that there must be no 'safe spaces' for terrorist funding at the G20 2017 talks. See *BBC*, 'May to Press G20 on Terror Financing', 7 July 2017; *Times of Israel*, 'Macron Calls for Global Cooperation to Cut Off Funds to Terrorists', 27 April 2018.

their networks and training camps and to mount attacks. Signing Executive Order 13224, then President George W Bush said: 'We will starve the terrorists of funding, turn them against each other, rout them out of their safe hiding places and bring them to justice'.[29] This statement was echoed 14 years later by former UN Secretary General Ban Ki-moon, who called on states to 'join forces to prevent [terrorists] from acquiring resources to do further harm'.[30] The use of economic disruption against terrorists remains a central component of current counterterrorism policies, but this approach only works where the financial activity undertaken by a terrorist group to sustain its operations is sizeable and vulnerable to external intervention. Given the genesis of the global CTF regime, this model reflects the approach developed as part of the response to the financial activity of Al-Qa'ida following the 9/11 attacks.

As long as terrorists remain faithful to their cause rather than use ideology as an excuse for simply profiteering, money is not an end in itself for them but rather a means to obtain necessary supplies and fund attacks. Accordingly, whereas 'financing' is convenient shorthand, since the early days of the global CTF regime promoted by the UN's 1999 convention, the focus of the international community should be on 'assets of every kind, whether tangible or intangible'.[31] In line with the CTF Convention, domestic legislation typically makes no distinction between giving terrorists money or other assets,[32] so that counterterrorist *financing* is and has always been to some extent a misnomer that has supported the popularisation of 'cutting off funding' as *the* CTF strategy.

One country that has considered this distinction – although not widely adopted in government publications[33] – is Canada, where there has been reflection on the policy implications of

29. The White House, 'President Freezes Terrorists' Assets', 24 September 2001.
30. UN, 'Unanimously Adopting Resolution 2253 (2015), Security Council Expands Sanctions Framework to Include Islamic State in Iraq and Levant', SC/12168, press release, 17 December 2015, <https://www.un.org/press/en/2015/sc12168.doc.htm>, accessed 29 December 2019.
31. UN, 'International Convention for the Suppression of the Financing of Terrorism', Article 1. See also FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: FATF Recommendations', Interpretive Note to Recommendation 5 (referring to 'funds or other assets'). See also, for example, 18 US Code §2339A (the criminalisation of 'material support' for terrorism in the US) and sections 15–17 of the Terrorism Act 2000 (referring to 'money or other property' in the UK).
32. See 18 US Code §2339A (the criminalisation of 'material support' for terrorism in the US) and sections 15–17 of the Terrorism Act 2000 (referring to 'money or other property' in the UK).
33. For instance, there was no mention of this point in House of Commons of Canada, 'Terrorist Financing in Canada and Abroad: Needed Federal Actions', Report of the Standing Committee on Finance, Second Session, 41st Parliament, June 2015.

focusing on terrorist *resourcing* rather than financing.[34] One law enforcement officer provided an example of terrorist resourcing as fuel used to drive a foreign terrorist fighter to the airport.[35]

This does not mean that the well-accepted terminology needs to be revised; merely that it should be emphasised that CTF policies need not be limited to reducing terrorist access to money alone. In line with the prevailing usage, this paper mostly refers to 'financing' and 'funds'. Unless the context requires otherwise, these terms should be treated as inclusive of all types of resources drawn upon by terrorist actors.

The objective of completely depriving terrorists of *all* resources, or *all* funds, is impossible to fulfil while the terrorists in question – and their supporters – remain active. As one US law enforcement officer stated, terrorism is an 'infinite game' that you cannot stop, as everyone in the network is replaceable.[36] Despite the occasionally hyperbolic language used by policymakers or journalists, CTF policies can be reasonably expected to deprive their targets of only *some* of their resources, or to make it as difficult as possible to use them.

Using Financial Intelligence to Detect and Disrupt Terrorist Networks

The second key pillar of CTF policies is the ambition to use financial intelligence in support of counterterrorism investigations. The value of this approach was emphasised in the Monograph on Terrorist Financing by the 9/11 Commission Staff, which observed that '[T]he current intelligence community approach appropriately focuses on using financial information, in close coordination with other types of intelligence, to identify and track terrorist groups rather than to starve them of funding'.[37]

Financial intelligence is therefore not the only type of intelligence that can be used to detect, investigate or prosecute terrorist financing, nor should it be confined to information provided to national financial intelligence units via a statutory suspicious transaction reporting regime. Other types of intelligence include physical evidence from the crime scene, human intelligence sources and covert observations.[38] Although 'following the money' requires the expertise

34. Minister of Public Works and Government Services, 'Air India Flight 182: A Canadian Tragedy', *Terrorist Financing* (Vol. 5, 2010) pp. 51–54, referring to John Schmidt's 'terrorist resourcing model'.
35. Authors' interview with Canadian law enforcement officer, Ottawa, October 2017; authors' interview with US law enforcement officer, Washington, DC, October 2017; UK law enforcement officer at the RUSI advisory board meeting, London, 1 March 2018.
36. Authors' interview with US law enforcement official, Washington, DC, October 2017.
37. Roth, Greenburg and Wille, 'National Commission on Terrorist Attacks Upon the United States', p. 7.
38. College of Policing, 'Intelligence Strategy', 23 October 2013, <https://www.app.college.police.uk/app-content/investigations/investigative-strategies/intelligence-strategy/>, accessed 29 December 2019.

of dedicated financial investigators, their work forms part of the overall investigatory effort. Accordingly, financial intelligence should be viewed as just one component of the investigatory toolbox. Furthermore, financial intelligence need not only be applied against terrorist *financing* but can support many other aspects of a terrorism investigation.

In the view of one senior intelligence officer, financial intelligence is not prioritised to the extent that it should be, notwithstanding the available technological capabilities for exploiting this form of intelligence. In the officer's view, the approach taken to the use of financial data is 'lagging', despite the fact that financial footprints are 'brighter than they have ever been', unlike communications data which is increasingly encrypted.[39] Thus, if financial intelligence is integrated and overlaid with other intelligence, it can be transformative.

Box 1: Terrorist Finance Tracking Program and the Use of SWIFT Data

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a cooperative society registered in Belgium that is co-owned by a number of banks and enables the communication of payment orders among more than 11,000 participating banks.[i] In October 2001, SWIFT began providing the US Treasury with information relating to batches of transactions it had processed.[ii] SWIFT did so on the basis of administrative subpoenas issued by the Treasury, which do not require judicial authorisation.[iii] The provision of information by SWIFT to the US Treasury became known as the Terrorist Finance Tracking Program (TFTP). The *New York Times* broke news of the programme in June 2006,[iv] which led to investigations of its legality in the EU.[v] In an attempt to reconcile the programme with EU law, the Council of the EU and the US drew up an agreement on the processing and transfer of SWIFT data in November 2009.[vi] However, the agreement failed to receive the approval of the European Parliament. A revised version was signed in July 2010 and entered into force the following month.[vii]

Notwithstanding the legal debate on ensuring that data is used and protected appropriately, the TFTP has provided examples of the valuable use of financial intelligence.

According to a Questions and Answers document produced by the US Treasury, 'since its inception in 2001, the TFTP 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 of the past decade'. The document cites a range of high-profile conducted and foiled attacks from across the globe in support of this assertion and also notes that 'a significant number of the leads generated by the TFTP have been shared with EU Member State Governments, with more than 2,000 such reports shared through February 28, 2014'.[viii]

i. SWIFT, 'Discover SWIFT', <https://www.swift.com/about-us/discover-swift?AKredir=true>, accessed 29 December 2019; SWIFT, 'Organisation & Governance', <https://www.swift.com/about-us/organisation-governance>, accessed 29 December 2019.

39. Authors' interview with senior Canadian intelligence officer, Ottawa, October 2017.

ii. Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare,* pp. 53–54.
iii. Justin Santolli, 'The Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive', *George Washington University International Law Review* (Vol. 40, 2008), pp. 553, 562.
iv. Eric Lichtblau and James Risen, 'Bank Data Is Sifted by U.S. in Secret to Block Terror', *New York Times*, 23 June 2006.
v. Belgian Privacy Commission, 'Opinion No. 37/2006 of 27 September 2006 Concerning the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST [OFAC] Subpoenas' (unofficial English translation), <https://www.steptoe.com/images/content/1/6/v1/1632/2644.pdf>, accessed 29 December 2019; European Data Protection Supervisor, 'EDPS Opinion on the Role of the European Central Bank in the SWIFT Case', 1 February 2007.
iv. Council of the European Union, 'Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the Signing, on Behalf of the European Union, 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 Purposes of the Terrorist Finance Tracking Program', *Official Journal of the European Union* (L 8/9, 13 January 2010).
vii. Council of the European Union, 'Council Decision (2010/412/EU) of 13 July 2010 on the Conclusion 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', *Official Journal of the European Union* (L 195/3, 27 July 2010).
viii. US Department of the Treasury, 'Terrorism Finance Tracking Program: Questions and Answers', <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/tftp_brochure_05062014.pdf>, accessed 7 October 2019.

CTF and Public–Private Partnerships

Information-sharing partnerships between the public and private sector[40] represent another way in which financial intelligence can be exploited, ensuring that law enforcement agencies (LEAs) benefit from the information held by regulated entities and, conversely, that regulated entities are attuned to the priorities of LEAs and appraised of relevant typologies. Compared to relying solely on information received via reporting by the private sector or from information disclosure requests made to financial institutions by LEAs, such partnerships have the advantage of enabling information sharing on a permanent basis and at the initiative of any of the participants. This more dynamic mode of information sharing enables greater agility in the recognition of and response to relevant financial crime risks, including terrorist financing.[41]

40. Due to their composition from both public and private bodies, such information-sharing partnerships are also often referred to as 'public–private partnerships' in this context.
41. See David Artingstall and Nick Maxwell, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017).

Financial intelligence has played a key role in facilitating investigations in the aftermath of terrorist attacks.[42] In the UK, the creation in 2015 of the Joint Money Laundering Intelligence Task Force (JMLIT), the UK's public–private–partnership between law enforcement and the financial sector, has boosted the extent to which these investigations can rapidly exploit financial intelligence.[43]

The JMLIT operates on two levels. There is an operational group supported by a series of expert working groups including a Terrorist Financing Expert Group (TFEG). The operational group, which addresses all forms of financial crime impacting the UK, brings together vetted representatives from UK retail and commercial banks, non-bank financial institutions (such as money-service businesses), the FinTech sector and law enforcement agencies to share information related to ongoing investigations. This sharing is facilitated by Section 7 of the Crime and Courts Act 2013, which provides an information-sharing gateway between the UK National Crime Agency (NCA) and the private sector.[44] The TFEG draws on a range of experts from industry and government to discuss emerging trends and share best practices, typologies and red-flag indicators, but not nominal or customer information.

In a similar vein, the Netherlands established a Terrorism Financing Taskforce in 2017 involving actors from the national police, the Public Prosecutor's Office, the Financial Intelligence Unit (FIU)-the Netherlands, several major banks and an insurer.[45] In this taskforce, the police and prosecutors share names with the private sector if there is an indication that a person is linked to terrorism. In one reported case, the taskforce determined how plane tickets to Syria were being financed using multiple bank accounts controlled by middlemen. According to Maarten Rijssenbeek, the former national coordinating prosecutor on terrorist financing, these transactions would not have been identified if the banks had not had access to the contextual information that was provided.[46]

At the international level, Europol has established a multi-country forum, the Europol Financial Intelligence Public Private Partnership (EFIPPP). Since its launch in December 2017, the breadth of its activities and the level of participation has increased consistently.[47] In Southeast Asia, as discussed later in this paper, since 2015 a regular series of cross-border partnership

42. Authors' interview with a bank compliance officer, London, January 2018.
43. For further information on JMLIT, see National Crime Agency, 'Improving the UK's Response to Economic Crime', <https://nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre>, accessed 20 August 2019.
44. Crime and Courts Act 2013 (UK).
45. Financial Intelligence Unit – the Netherlands, 'Annual Report 2017', <https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/7238-fiu_jaaroverzicht_2017_eng_web_1.pdf>, accessed 30 December 2019.
46. Ruben Munsterman, 'Dutch Banks Mix With Cops, Prosecutors in Bid to Fight Terrorism', *Bloomberg*, 18 July 2018.
47. Council of the European Union, 'JHA Agencies' Role in Counter-Terrorism', 27 February 2018, <http://data.consilium.europa.eu/doc/document/ST-6146-2018-INIT/en/pdf>, accessed 7 October 2019.

meetings targeting terrorist financing have been established under the flagship Southeast Asia CTF Summit.[48]

Such partnerships do not always involve the sharing of nominal data, as practised in the UK and the Netherlands where the partnership models benefit from a legal underpinning for information sharing. Typology-based public–private partnerships that discuss trends, red flags and best practices can be highly effective in building trust, awareness and systemic integrity. For example, Singapore's AML/CFT Industry Partnership (ACIP),[49] established in April 2017 on this basis, demonstrates the benefits of bringing together banks, regulators, LEAs and other relevant actors to discuss the financial crime risks faced by Singapore and the surrounding region.[50]

Recommendations

With a few notable exceptions, research for this paper indicates that for most actors and agencies focused on CTF, responses are rooted in the first of the two approaches discussed above, aiming to identify and 'cut off' funding that supports terrorist groups. As this paper will next explore, while such an approach may be appropriate – and somewhat achievable due to the more exposed nature of financial activity – when targeting the funding of a large group such as ISIL or Al-Qa'ida, this approach is not appropriate for actors that require little or no funding to mount attacks or are related to a larger group but are acting outside their core territory. In these cases, this paper argues that greater reliance should be placed on exploiting the intelligence value of finance.

Before considering how CTF responses should be shaped to match specific forms of risk, this paper first offers some recommendations as to how the conceptual approach to this financing can be enhanced.

Make Greater Use of Financial Intelligence

- Recognise that CTF measures should focus not only on depriving terrorists of funds, but also on using financial intelligence against them to the best effect.
- The use of financial intelligence should be integrated with more commonly exploited intelligence sources.

48. For further details, see Australian Government, 'AUSTRAC: International Partners', <https://www.austrac.gov.au/about-us/international-engagement/international-partners>, accessed 7 October 2019.
49. Association of Banks in Singapore, 'AML/CFT Industry Partnership, ACIP', <https://abs.org.sg/industry-guidelines/aml-cft-industry-partnership>, accessed 30 December 2019.
50. The issue of public–private partnerships and financial crime are explored in detail by RUSI in the following two papers: Maxwell and Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime'; Nick Maxwell, 'Expanding the Capability of Financial Information-Sharing Partnerships', *RUSI Occasional Papers* (March 2019).

Use Financial Intelligence in at Least Four Distinct Ways

- To identify relationships and the extent and participants of terrorist networks.
- To identify suspicious behaviour that may be in support of a terrorist group or indicate an intent to commit a terrorist act.
- To reconstruct the sequence of events leading to a terrorist attack based on the suspect's financial activities.
- To support non-financial aspects of a terrorism investigation.

Financial intelligence should become a more central element of counterterrorism responses, leveraging the capabilities and data of domestic FIUs, national and regional security bodies and the transaction-monitoring capacity of the private sector. International cooperation to facilitate the cross-border sharing of financial intelligence should likewise be promoted and barriers to such sharing identified and addressed.[51]

Finally, it should be recognised that in an era where communications data is increasingly encrypted, financial intelligence offers a potentially rich and exploitable data-source that can supplement and enhance the tools traditionally favoured to support counterterrorism responses.

Promote Collaboration

- Between counterterrorism and law enforcement officials.
- Between public and private sectors.
    - Consider models such as the UK JMLIT terrorist financing expert working group and the Netherlands Terrorist Financing Taskforce.
- Between countries and within regions.
    - Consider models such as the Southeast Asia CTF Summit, the Europol Financial Intelligence Public Private Partnership, and counter Hizbullah initiatives such as the Law Enforcement Co-ordination Group (LECG)[52] and Counter-Hizballah International Partnership (CHIP).[53]

Cooperation between the public and private sectors can lead to an overall increase in terrorist-financing awareness, understanding and higher-quality suspicious transaction reporting to law enforcement. In jurisdictions the authors visited for this project, a strong relationship between the public and private sector manifested in a variety of forms, including through interpersonal relationships between private sector and law enforcement partners; cross-sector groups that had the ability to share nominal data; and cross-sector groups that discussed risks, trends, typologies and disseminated terrorist financing indicators. This, in the words of one FIU director, resulted in an 'immediate increase in the quality of terrorist-financing-related STRs

51. For an extensive discussion of the barriers to cross-border information sharing see *Ibid*.
52. Levitt, 'America May Have Unlocked a Key to Fighting Terrorism – And it Doesn't Involve Drones'.
53. US Department of the Treasury, 'Treasury Launches the Counter-Hizballah International Partnership [CHIP] to Thwart Illicit Financial Activity'.

[suspicious transaction reports]'.[54] Cross-border partnerships such as Europol's EFIPPP and those fostered by the Southeast Asia CTF Summit have the potential to further strengthen the global CTF regime.

Governments should not limit partnerships to the formal banking sector. Since 9/11, terrorist financing has operated primarily outside this sector, taking advantage of lower compliance standards in remittance companies and the fundraising and fund-moving opportunities presented by the charitable sector. Furthermore, as technology-enabled financial services develop, FinTech payments companies, social-media and communication-service providers play an increasingly important role in combating terrorist financing and supplying valuable financial intelligence.

Identify and Engage with Key Terrorist-Resource Suppliers

Policymakers should acknowledge more clearly that an effective CTF regime is not only about finance itself, but also about the *resources* on which the funds are spent. Domestic legislation typically makes no distinction between providing designated or prospective terrorists with money or other assets. The information held by non-financial sectors regarding their customers may also enhance the law enforcement intelligence picture. Therefore, CTF knowledge and best practice should be shared and disseminated with other appropriate sectors. For example, the prevalence of vehicle-based attacks in Europe suggests that companies that hire or sell equipment such as cars and vans that can be used in terrorist attacks could contribute valuable intelligence to counterterrorism efforts. Additionally, law enforcement should cultivate relationships with key players in these industries in their jurisdictions, encouraging them to report indications of activity that raises suspicions of attack planning.

54. Authors' interview with the director of an FIU, Middle East, February 2019.

II. Risk Profile

A CORE FINDING OF the research for this paper is that CTF regimes often lack a foundation in the specific risk faced by an individual country or region. Where a CTF regime is identifiable, it is often rooted in the post-9/11 approach developed by the international community to combat Al-Qa'ida, which may not align with the risk a country currently faces, or indeed faced in the past.

The profile of terrorist actors ranges from small cells or lone actors – who may be self-motivated or may be directed or inspired by a group such as Islamic State – to large territory-controlling groups or groups that span continents with financial management and fundraising capabilities to match. While Al-Qa'ida under Osama bin Laden was also an efficient fundraising organisation, its focus on donations and deep-pocketed donors contrasts, as this chapter explores, with the methods employed more commonly by large terrorist groups today.

As will be discussed in this chapter, this diversity of profile is reflected in the varying ways in which terrorist actors raise, move, store and spend funds; it also poses challenges for policymakers. A 'one-size-fits-all' approach to terrorist financing risks being ineffective. The nature of the risk needs to be properly understood, including its financing modus operandi, before a CTF strategy can be developed and implemented.

This chapter therefore seeks to explore this approach to CTF by dividing terrorist actors into three primary categories, along lines determined by shared financing characteristics, which should in turn inform the creation of an appropriate CTF strategy:

- Territory-controlling groups.
- Organised crime-type groups (hereafter, OCG-type groups).
- Small cells and lone actors (whether directed, inspired or self-motivated).

The distinctions between these different groups are a matter of degree, with blurred dividing lines. For instance, an OCG-type group operating fundraising businesses may also benefit from controlling forms of territory such as city neighbourhoods or communities. By the same token, whether a given group is properly viewed as a small cell or part of an OCG-type group can often be debated. The objective of this classification is not to assign precisely defined labels to each terrorist actor but to provide a starting point for thinking about the CTF measures that may be most effective in relation to such an actor.

Over their lifespan, terrorist groups can move from one category to another. For instance, in January 2018, the UN Secretary General Antonio Guterres warned that '[having] lost its focus on conquering and holding territory, ISIL is now organised as a global network, with a flat hierarchy

and less operational control over its affiliates'.[55] ISIL's mutation as a result of extensive territory loss leaves the international community with important questions regarding what happened to the large sums of money it accrued at the height of its powers. According to experts, as Islamist militants retreated from Iraq and Syria, they carried with them an estimated $400 million in Western and Iraqi currency and gold coins.[56] Much of this is believed to have been laundered through legitimate businesses across the Middle East. For example, a counterterrorism official in the Kurdistan Regional Government's CT Department reportedly stated that 'They [ISIL] continue to fund terrorist activity. They also use money to pay the salaries of fighters and to support their families. Some of it even goes to pay for lawyers to help their people who are in prison'.[57] Inevitably, as a terrorist group is squeezed, its operations, including its financial strategy, will adapt, forming a crucial element in the overall strategy by which it can regroup and survive. The CTF response needs to anticipate this change and adapt accordingly.

Furthermore, a terrorist actor may display the characteristics of one category in one country but those of a different category elsewhere. For example, ISIL controlled large swathes of territory in Iraq and Syria while at the same time operating through directed small cells,[58] inspiring lone actors,[59] and encouraging affiliates in other parts of the Middle East, Southeast Asia and West Africa.[60] It is therefore imperative for policymakers to consider the specific characteristics of terrorist actors in the location in which they operate.

The development of CTF measures is often event-driven, such as the rapid advancement of the international CTF regime after 9/11. A clear understanding of the risk at hand and the means by which the threat is funded should lead to considered rather than knee-jerk CTF responses. As one policymaker noted, many jurisdictions in his region 'lack national CTF policies

55. UN Security Council, 'Sixth Report of the Secretary-General on the Threat Posed by ISIL to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat', S/2018/80, 31 January 2018, para. 6. For a similar assessment, see Financial Transactions and Reports Analysis Center of Canada (FINTRAC), 'Terrorist Financing Assessment 2018', December 2018, p. 8.
56. Colin P Clarke, 'ISIS's New Plans to Get Rich and Wreak Havoc', *Foreign Policy*, 10 October 2018.
57. Joby Warrick, 'Retreating ISIS Army Smuggled a Fortune in Cash and Gold Out of Iraq and Syria', *Washington Post*, 21 December 2018.
58. For example, the November 2016 Paris attacks. See *BBC*, 'Paris Attacks: What Happened on the Night', 9 December 2015.
59. For example, Khalid Masood, the Westminster Bridge attacker in 2017. See *BBC*, 'London Attack: Who was Khalid Masood?', 26 March 2017.
60. For example, ISIS in Afghanistan. See *Al Jazeera*, 'ISIL Expands its Reach into Afghanistan, Threatening the West', 10 June 2019; Counter Extremism Project, 'Boko Haram', <https://www.counterextremism.com/threat/boko-haram>, accessed 19 September 2019; for ISIS in the Philippines see Hannah Beech and Jason Gutierrez, 'How ISIS is Rising in the Philippines as it Dwindles in the Middle East,' *New York Times*, 9 March 2019.

that are informed by the identified risks'.[61] The next section emphasises the importance of context-specific responses to terrorist financing.

Territory-Controlling Groups

For the purposes of this paper, a territory-controlling terrorist group is one that succeeds in establishing control over an area for an extended period of time to the exclusion of other significant actors, such as government forces or competing groups, and derives resources sufficient to ensure its survival, for example by exploiting natural resources or taxing the population under its control.[62]

Controlling territory allows a group to achieve a significant degree of financial self-sufficiency and therefore minimise its need to rely on external support. The financial opportunity is enhanced if the territory in question contains key trade routes or ports that can be exploited to generate further revenue.

For instance, over time, the Islamist insurgency Al-Shabaab has controlled various parts of Somalia, including key revenue-earning districts of Mogadishu (such as the Bakara Market), as well the port city of Kismayo (a gateway for the Somali charcoal export business), which has been vital to the funding of its operations.[63] Despite losing much of its territory after an African Union-led offensive in 2011–12, Al-Shabaab continues to hold swathes of rural land, and with it ,fundraising opportunities.[64] As noted by the UN, territorial control enables the group to 'derive its revenue from a variety of domestic sources, primarily taxation on transiting vehicles and goods, business and agricultural taxation, and forced *zakat* [alms] levies'[65] as well as raising funds from territory it does not physically control.[66]

61. Authors' interview with financial crime policymaker, Kathmandu, July 2018.
62. In this context, taxation and extortion are synonymous given that terrorist groups in control of a territory have no recognised legal authority to levy taxes.
63. US House of Representatives Committee on Financial Services, the Task Force to Investigate Terrorism Financing, 'Stopping Terror Finance: Securing the U.S. Financial Sector', 20 December 2016, p. 14; see also Tom Keatinge, 'The Role of Finance in Defeating Al-Shabaab', *Whitehall Report*, 30 December 2014.
64. US Department of State, 'Country Reports on Terrorism 2017 – Foreign Terrorist Organizations: Al-Shabaab', 19 September 2018, <https://www.refworld.org/docid/5bcf1f57a.html>, accessed 6 September 2019.
65. Kairat Umarov, 'Letter Dated 7 November 2018 from the Chair of the Security Council Committee Pursuant to Resolutions 751 (1992) and 1907 (2009) Concerning Somalia and Eritrea Addressed to the President of the Security Council', S/2018/1002, 9 November 2018, p. 25, para. 82.
66. Somalia UN Panel of Experts Report, 2019, p. 3.

Other groups that have at various points relied on territorial control to finance their operations include Boko Haram in northeastern Nigeria,[67] Islamic State in Iraq and Syria,[68] and the FARC up until 2016.[69] In order to sustain the activities necessary to maintain control over territory and provide the expected services to the population – even if the controlled businesses and population welcome this – considerable funding is needed in contrast to maintaining an insurgency campaign. This requires an effective system for collecting and managing revenue that may resemble, or surpass, the tax and revenue collection practices adopted by recognised governments. In the case of Somalia, the UN notes that 'Al-Shabaab's domestic revenue generation apparatus is more geographically diversified and systematic than that of the Federal Government or the federal member states'.[70]

Similarly, at the height of its territorial control, when the group was believed to have annual earnings of $1–2 billion,[71] Islamic State was reported to have developed a well-functioning taxation system that supplemented its income from oil sales to opportunistic networks who made use of pre-existing smuggling routes and may have benefited from their supposed proximity to Syrian authorities.[72] Reporting from 2015 suggests that Islamic State was 'exacting tolls and traffic tickets; rent for government buildings; utility bills for water and electricity; taxes on income, crops and cattle; and fines for smoking or wearing the wrong clothes'.[73] The importance of this revenue stream and the impact of coalition airpower targeting oil revenue assets meant that by 2016 the income Islamic State derived from taxation in Syria reportedly surpassed that from oil sales by 6:1.[74]

67. The Home Office, 'Country Policy and Information Note: Nigeria: Boko Haram', version 2.0, January 2019, p. 16.
68. FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant', February 2015.
69. Canada: Immigration and Refugee Board of Canada, 'Colombia: The Revolutionary Armed Forces of Colombia (*Fuerzas Armadas Revolucionarias de Colombia*, FARC), Including Demobilization of Former Combatants; Information on Dissident Groups, Including Number of Combatants, Areas of Operation, Activities and State Response (2016–April 2018)', 18 April 2018, <https://www.refworld.org/docid/5afad95e4.html>, accessed 6 September 2019.
70. Umarov, 'Letter Dated 7 November 2018 from the Chair of the Security Council Committee Pursuant to Resolutions 751 (1992) and 1907 (2009) Concerning Somalia and Eritrea Addressed to the President of the Security Council', p. 26, para. 86.
71. Colin P Clarke et al., *Financial Futures of the Islamic State of Iraq and the Levant: Findings from a RAND Corporation Workshop* (Santa Monica, CA: RAND Corporation, 2017); Agnès Levalloise, *The Financing of the 'Islamic State' in Iraq and Syria* (Brussels: European Parliament, Directorate-General for External Policies, 2017), p. 8.
72. FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant', p. 14.
73. Matthew Rosenberg, Nicholas Kulish and Steven Lee Myers, 'Predatory Islamic State Wrings Money From Those It Rules', *New York Times*, 29 November 2015.
74. Rukmini Callimachi, 'The ISIS Files: When Terrorists Run City Hall', *New York Times*, 4 April 2018.

Territory-controlling groups operate like a state in other ways,[75] for instance by maintaining a semblance of social order and providing services, such as health services, to the population.[76] Thus, the ability of groups in this category to control territory and garner related revenue sets them apart from the other types of terrorist actor considered later in this section.

While the size of the territory controlled by a terrorist group can differ, what matters is the continuing ability to exert authority over and extract rent from a territory. As academic Jodi Vittori notes, such a group 'will stand until some stronger group comes along, such as a rival terrorist faction or warlord, a newly invigorated local government, or a foreign power'.[77]

Fundraising Methods

The typical generation of income by territory-controlling groups can be divided as follows:

- Income generated within the controlled territory, such as:
    - Trade in natural resources, such as oil, metals and minerals.
    - Trade in agricultural and timber products.
    - Trade in other licit and illicit commodities, including drugs.
    - Taxation of trade routes, including those used by criminals.
    - Taxation/extortion of the population including kidnap-for-ransom.

- Income generated from outside the controlled territory, such as:
    - Donations.
    - Funds brought by incoming terrorist fighters.
    - Involvement in criminal activities, such as drug trafficking.
    - Legitimate business.
    - State support.

Internal Income

Maximising income generated from territorial control can provide terrorist groups with considerable operational security. In the case of the Islamic State, virtually all the group's

75. It is worth noting that by controlling territory, not only does a terrorist group boost its revenue potential but it also increases its costs (and thus the need to raise funding) as those under its control expect services and security that at least match those that existed before.
76. Callimachi, 'The ISIS Files'.
77. Jodi Vittori, *Terrorist Financing and Resourcing* (New York, NY: Palgrave Macmillan, 2011), p. 8.

revenue was generated internally.[78] Depending on the role that terrorist-controlled territory plays in the supply chain, terrorists can profit by:[79]

- Extracting natural resources and selling them to companies that further transport and resell them.
- Levying taxes on companies that directly engage in extraction.
- Taxing trade and smuggling routes.
- Refining and selling illegally extracted resources.

According to FATF, sectors such as oil, gas, timber, diamonds, charcoal and precious metals have historically been vulnerable to exploitation by terrorist groups.[80] Al-Shabaab provides a fitting example. According to UN figures published in November 2018, the tax levied at checkpoints on the trade in charcoal provided the group with at least $7.5 million in the previous year.[81] This is despite the 2012 UN ban on charcoal exports from Somalia.[82] The UN provides the following account of the mechanics of the trade:

> [T]he principal initial destination ports for Somali charcoal were the Kish free zone and the Qeshm free zone in the Islamic Republic of Iran … The process involved using false certificates of origin from the Comoros, Côte d'Ivoire and Ghana to import Somali charcoal, repackaging the charcoal from typical blue-green bags into white bags labelled as "Product of Iran". The bags were then reloaded onto smaller, Islamic Republic of Iran-flagged dhows, and exported to Hamriyah port, Dubai, United Arab Emirates, using certificates of origin falsely indicating the country of manufacture of the charcoal as the Islamic Republic of Iran.[83]

In Afghanistan, the UN reported that in 2019 the Taliban continued to generate income through illicit mineral and other resource extraction, providing the example of marble quarries in Helmand that remain under the direct control or strong influence of the group. The lack of government control in certain areas facilitated and exacerbated this exploitation by territory-controlling groups. Revenue for Islamic State in Afghanistan similarly comes from

78. For example, see Center for the Analysis of Terrorism, 'ISIL Financing 2015', May 2016, p. 7; UN Security Council, 'Second Report of the Secretary-General on the Threat Posed by ISIL to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat', S/2016/501, 31 May 2016, paras. 9–12.
79. OECD, 'Terrorism, Corruption and the Criminal Exploitation of Natural Resources', October 2017, p. 4.
80. FATF, 'Emerging Terrorist Financing Risks', October 2015, p. 39.
81. Umarov, 'Letter Dated 7 November 2018 from the Chair of the Security Council Committee Pursuant to Resolutions 751 (1992) and 1907 (2009) Concerning Somalia and Eritrea Addressed to the President of the Security Council', p. 6.
82. UNSCR 2036, 22 February 2012, para. 22.
83. Umarov, 'Letter Dated 7 November 2018 from the Chair of the Security Council Committee Pursuant to Resolutions 751 (1992) and 1907 (2009) Concerning Somalia and Eritrea Addressed to the President of the Security Council,' p. 45, para. 175.

the exploitation of local resources, including illegal mining, timber logging and the extortion of transportation resources.[84]

A further example of rent seeking is provided by the New People's Army (NPA), the armed wing of the Communist Party in the Philippines,[85] notorious for exacting 'revolutionary taxes' within the territory it occupies. The Philippines' military has estimated that the NPA collects PHP460 million ($8.7 million) annually.[86] The Philippines' 2017 National Risk Assessment on Money-Laundering and Terrorist Financing underlined that groups active in the country, including the Abu Sayyaf Group, Maute Group and the NPA, collected from residents, local businesses, bus companies that passed through their controlled areas and larger companies such as mining firms, construction firms and telecommunications companies.[87] According to a senior Philippines government official, businesses which did not pay may face arson attacks on their estates, burning of buses or pulling down of mobile network masts.[88]

Many other examples of territorial exploitation exist, from the FARC and the Taliban raising income from cultivating and selling narcotic substances,[89] to the misappropriation of property through robberies and racketeering by Boko Haram,[90] and allegations of involvement in the drugs- and arms-trade by the Movement of Democratic Forces of Casamance in Senegal.[91] The

84. Dian Triansyah Djani, 'Letter Dated 10 June 2019 from the Chair of the Security Council Committee Established Pursuant to Resolution 1988 (2011) Addressed to the President of the Security Council', S/2019/481, 13 June 2019.
85. Note that although the US designated the NPA as a terrorist organisation in 2002, the Philippines only designated the group in 2018. See Republic of the Philippines Anti-Money Laundering Council (AMLC), 'Second National Risk Assessment on Money Laundering and Terrorist Financing', 2017, p. 289.
86. Frinston Lim, 'Military Says NPA Collects P460M Yearly as "Revolutionary Taxes"', *Inquirer.Net*, 13 December 2017.
87. Republic of the Philippines AMLC, 'Second National Risk Assessment on Money Laundering and Terrorist Financing', p. 290.
88. Authors' interview with senior Philippine government official, Manila, February 2018.
89. FARC was widely reported to benefit from taxing the production of drugs or selling drugs itself. See, for example, Zarate, *Treasury's War*, p. 369; Thomas R Cook, 'The Financial Arm of the FARC: A Threat Finance Assessment', *Journal of Strategic Security* (Vol. 4, No. 1, 2011). However, assessments of the monetary value that FARC thus generated vary widely. See John Otis, 'The FARC and Colombia's Illegal Drug Trade', Wilson Center Latin America Program, November 2014, pp. 8–13. In relation to the Taliban, the UN Al-Qa'ida and Taliban Sanctions Monitoring Team reported that one-third of its income in 2011/12 derived from the poppy trade. See FATF, 'Emerging Terrorist Financing Risks', p. 16. Some estimates put the Taliban's annual income from drug trade at $70–$400 million. See Zarate, *Treasury's War*, p. 369.
90. FATF, GIABA and GABAC, 'Terrorist Financing in West and Central Africa', October 2016, p. 11.
91. GIABA, 'The Nexus Between Small Arms and Light Weapons and Money Laundering and Terrorist Financing in West Africa', 2013, para. 78.

engagement by terrorist groups, including those that control territory, in illicit trafficking is often cited as a manifestation of the 'crime–terror nexus' that is discussed further in this section.[92]

External Income

Given this paper's focus on preventing terrorist financing, in this case 'external income' refers to funds that a terrorist group raises or receives from outside its area of control and therefore needs to move. In particular, this need to move funds creates opportunities for law enforcement interventions not available against internally generated funds.

In some instances, terrorists are able to generate funds from criminal activity or infiltration of legitimate businesses in areas adjacent to the territory they control, especially if those spaces are contested or do not benefit from strong government control. One example is Boko Haram 'provid[ing] microfinance to small and medium scale businesses, in turn creating an investment network and increasing the organisation's financial stability'.[93]

Terrorist groups can also look further afield to raise funds. FATF cites a designation by the US Treasury of an '[Islamic State] official who received a 2 million USD donation emanating from the Gulf';[94] the Liberation Tigers of Tamil Eelam (LTTE) was known to have solicited and extorted donations from members of the Tamil diaspora in the UK and Canada;[95] and the National Risk Assessment of Terrorist Financing, published by the US Treasury in 2015, cites an FBI-led operation that disrupted the solicitation of donations for Al-Shabaab in the US. According to the report:

> These individuals used a variety of methods to raise funds for Al-Shabaab, including door-to-door personal solicitations and teleconferences. Although the amount raised by these individuals was not substantial compared to other terrorist financing cases (each sent approximately $16,000 to Somalia), it was considered an important revenue source by Al-Shabaab's leadership, which routinely directly communicated with the fundraisers.[96]

All terrorist groups, including territory-controlling ones, may benefit from external state sponsorship. Allegations of state sponsorship are normally highly controversial given the gravity

92. Tuesday Reitano, Colin Clarke and Laura Adal, 'Examining the Nexus Between Organised Crime and Terrorism and its Implications for EU Programming', CT-MORSE Consortium, 2017, pp. 13–15; US House of Representatives Committee on Financial Services' Task Force to Investigate Terrorism Financing, 'A Dangerous Nexus: Terrorism, Crime and Corruption', 21 May 2015.
93. FATF, Inter-Governmental Action Group Against Money Laundering in west Africa (GIABA) and Task Force on Money Laundering in Central Africa (GABAC), 'Terrorist Financing in West and Central Africa', p. 16.
94. FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)', p. 18.
95. Human Rights Watch, 'Funding the Final War: LTTE Intimidation and Extortion in the Tamil Diaspora', 14 March 2006.
96. US Department of the Treasury, 'National Terrorist Financing Risk Assessment', p. 42.

of the accusation. The US maintains a publicly available list of state sponsors of terrorism.[97] An oft-cited allegation of state sponsorship is Iran's support for Hizbullah, including the training of Hizbullah affiliates and providing funds.[98] In an ongoing dispute before the International Court of Justice, Ukraine has accused Russia of financing terrorism, in breach of the CTF Convention. As noted earlier, Article 2 of the CTF Convention covers 'assets of every kind', in this case the supplying by Russia of heavy artillery and other military equipment across the Ukraine–Russia border to the Donetsk and Luhansk People's Republic insurgent groups,[99] Russia denies the allegations.[100]

Movement of Funds

Internal Movement

Depending on the size of the controlled territory and the complexity of its administration, some internal movement of funds will be necessary in order to, for instance, allocate funds obtained from taxation towards the provision of various social services. Such movement is likely to take the form of:

- Transporting cash.
- Transferring funds through banks.[101]
- Transporting goods.

As discussed later, opportunities – if they exist – for disruption in relation to internal movement of funds typically take the form of military action against key nodes of the terrorist group's financial infrastructure, for example, cash storage sites or transportation routes and convoys.

External Movement

In contrast with the other forms of terrorist actor discussed in this chapter, the importance of external movement of funds is attenuated for groups that are largely self-sufficient by virtue of

97. US Department of State, 'State Sponsors of Terrorism', <https://www.state.gov/state-sponsors-of-terrorism/>, accessed 30 December 2019;
98. US Department of State, 'Countering Iran's Global Terrorism', 13 November 2018, <https://www.state.gov/countering-irans-global-terrorism/>, accessed 3 February 2020.
99. Terrorism Financing and Racial Discrimination in Ukraine (Ukraine v. Russia), Application Instituting the Proceedings of 16 January 2017, ICJ, paras. 45–46.
100. See the transcript of Russia's pleadings: <//www.icj-cij.org/files/case-related/166/166-20170309-ORA-01-00-BI.pdf>, accessed 30 December 2019.
101. As highlighted by FATF, banks operating elsewhere should cut their ties with banks in terrorist-controlled territories so as not to be used for terrorist financing. See FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)', p. 6. However, it be cannot ruled out that banks located in such territory will continue operating within its confines. See Yaya Fanusie and Landon Heid, 'What ISIS is Banking on', *Forbes*, 17 June 2016.

their territorial control. That said, possible reasons for moving funds in or out of the controlled territory include:

- Receiving donations from overseas (inward movement of funds).
- Transferring funds overseas to support affiliates for operational activity, or for investment (outward movement of funds).

The potential abuse by terrorists of not-for-profit organisations (NPOs, FATF's preferred term for charities) to support the inward movement of funds has been widely reviewed and debated.[102] Formal banking links of terrorist-controlled areas to the rest of the world are typically constrained and thus charities can offer an alternative means of moving funds and resources into areas where terrorists operate.[103] According to FATF, charities operating in geographical proximity to areas of terrorist activity face higher risks of being abused for terrorist financing.[104] In addition to the risk of legitimate charities being abused, bogus charities may be set up specifically for the purpose of moving terrorist funds. One such case was detected in the Netherlands due the fact that several charities and foundations that did not share similar goals, but were chaired by the same individual, and made transfers to individuals who were subsequently found to have travelled to Syria.[105] A consequence of the focus on charities as a vehicle for terrorist financing has been widespread de-risking of the sector, that is to say, the closure by banks of accounts that they fear might expose them – however remotely – to terrorist-financing risk.[106]

While the value of the inward flow of funds to a territory-controlling organisation is likely to be of modest importance in comparison to its other sources of income, an outward flow of funds may be critical to provide funding for an overseas-based affiliate to develop its operations and carry out attacks.

The need to invest funds abroad is another reason why a territory-controlling group may feel compelled to move money elsewhere. The UN has previously noted that 'Al-Shabaab is likely generating a significant budgetary surplus [and] [h]ow Al-Shabaab channels excess revenue remains under investigation by the Monitoring Group'.[107] Similarly, in August 2018, the UN Secretary General Antonio Guterres made the following observations about Islamic States's

102. FATF, 'Risk of Terrorist Abuse on Non-Profit Organisations', June 2014; Rodger Shanahan, 'Charities and Terrorism: Lessons from the Syrian Crisis', The Lowy Institute, 14 March 2018; Tom Keatinge, *Uncharitable Behaviour* (London: Demos, 2014).
103. *BBC*, 'Syria Aid Convoys: Two Guilty over Terror Funding', 23 December 2016.
104. FATF, 'Emerging Terrorist Financing Risks', p. 14.
105. *Ibid*, p. 15.
106. De-risking describes the loss of access to financial services by those customers that banks deem to pose too high a financial crime risk and that have their accounts closed. This issue has particularly affected charities operating in jurisdictions proximate to designated terrorist organisations.
107. Umarov, 'Letter Dated 7 November 2018 from the Chair of the Security Council Committee Pursuant to Resolutions 751 (1992) and 1907 (2009) Concerning Somalia and Eritrea Addressed to the President of the Security Council', p. 26, para. 84.

modus operandi in the wake of its military setbacks: 'ISIL members have reportedly invested in the region and infiltrated businesses, such as construction companies, money exchanges and agricultural, fisheries and real estate ventures, including hotels'. There is concern about ISIL financial facilitators and networks moving their operations to nearby countries.[108]

Typical methods that can be used to move funds by territory-controlling groups include:

- Methods involving the formal financial sector, such as:
  - Abuse of the formal banking system.
  - Use of mobile money and remittance companies.
  - Trade-based money laundering.[109]

- Methods not involving the formal financial sector, such as:
  - *Hawala* remittances.[110]
  - Cash smuggling.
  - Smuggling of goods, especially natural resources and high-value products (such as precious metals and antiquities).

Multiple means of moving funds are typically employed. For instance, Al-Shabaab reportedly 'collects revenues and conducts internal transfers using cash (both United States dollars and Somali shillings), mobile money, hawala money transfer and possibly bank accounts'.[111] The 2019 UN Somalia Panel of Experts report underlines this point, noting that: 'The group also continues to take advantage of virtually unregulated mobile money and domestic banking services to collect and transfer revenues through the country'.[112] Methods used by ISIL varied according to

108. UN Security Council, 'Seventh Report of the Secretary-General on the Threat Posed by ISIL to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat', S/2018/770, 16 August 2018, para. 17.
109. Trade-based money laundering is defined by FATF as 'the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origin'. See FATF, 'Trade-Based Money Laundering', 23 June 2006, p. 3. Trade-based money laundering involves the abuse of the financial system if money transfers are made to pay for the goods in question. In contrast, the smuggling of goods tends to involve no payments and therefore does not rely on the use of the financial system.
110. *Hawala* is a traditional form of money transfer that is highly effective for moving money into areas where formal banking and other remittance services do not operate. For an explanation of the workings of *hawala*, see Martin S Navias, *Finance & Security: Global Vulnerabilities, Threats and Responses* (London: C Hurst & Co, 2019), pp. 97–102.
111. Umarov, 'Letter Dated 7 November 2018 from the Chair of the Security Council Committee Pursuant to Resolutions 751 (1992) and 1907 (2009) Concerning Somalia and Eritrea Addressed to the President of the Security Council', p. 27, para. 89.
112. UN Security Council, 'Letter Dated 1 November 2019 from the Chair of the Security Council Committee Pursuant to Resolution 751 (1992) Concerning Somalia Addressed to the President of the Security Council', S/2019/858, 1 November 2019.

requirement. For example, some suggest that 'ISIL is not using the formal financial system, but rather storing its money internally and relying on an informal system of couriers and hawaladars – people who operate hawalas – to move it around'.[113] Its money is also 'infiltrating legitimate businesses in the region by using fronts, such as ostensibly "clean" individuals who can access the formal financial system'.[114]

International transfers – particularly via the formal financial system where transactions are screened and monitored – should represent a moment of particular vulnerability for terrorism funding. Collaborative working within regions or focused on specific terrorist risks is increasing knowledge in this regard, but continued improvements in the understanding of how groups move funds internationally must be made to facilitate the development of more effective interventions.

Storage and Investment

Since territory-controlling terrorist groups will at times generate excess funds, they require a means of preserving and storing them. In contrast, small cells and lone actors rarely have excess funds to store.[115] In short, there are three primary ways of storing funds that terrorists are likely to use, depending on the circumstances:

- Investment in, establishment of or taking control of businesses operating in the territory.
- Bulk cash storage.
- Hoarding of goods, including natural resources and other valuable commodities.

Terrorist groups may store considerable amounts in cash. For instance, ISIL was believed to have seized the equivalent of more than $500 million from Iraqi banks and kept the cash in bank vaults.[116] In May 2016, the UN Secretary General Ban Ki-moon predicted that, faced with the destruction of cash storage sites through US airstrikes, Islamic State would seek to invest funds into commodities such as gold.[117]

113. US House of Representatives Committee on Financial Services, 'Stopping Terror Finance: Securing the U.S. Financial Sector', p. 31.
114. UN Security Council, 'Sixth Report of the Secretary-General on the Threat Posed by ISIL [Da'esh] to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat', para. 14.
115. Emilie Oftedal, 'The Financing of Jihadi Terrorist Cells in Europe', Norwegian Defence Research Establishment (FFI), 6 January 2015, p. 8.
116. FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)', p. 12; Clarke et al., *Financial Futures of the Islamic State of Iraq and the Levant,* p. 12.
117. UN Security Council, 'Second Report of the Secretary-General on the Threat Posed by ISIL to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat', para. 14.

As with other aspects of territory-controlling groups' operations, their ability to store value in cash or goods is largely a corollary of their territorial control. At the same time, their attempts to move value outside that territory for storage purposes and, for instance, invest funds in legitimate businesses, present opportunities for disruption.

CTF Responses

A territory-controlling group by definition operates – in practice, although not in law – beyond the reach of any state's law enforcement. Opportunities for bringing terrorists to account by means of a judicial process or confiscating their property are therefore nugatory until legitimate government forces regain control and the group thus ceases to be territory-controlling. Although the use of sanctions is perhaps symbolically important, they are of limited direct effect as the freezing of assets and blocking of transactions that typically accompanies them will not impact their targets. Some argue that sanctions – in the form of secondary sanctions – do play a role against territory-controlling groups[118] as they are 'designed to inhibit non US citizens and companies abroad from doing business with a target of primary US sanctions'.[119] Technically, this may be the case, but it is not obvious that such sanctions have materially impacted the finances or operations of such groups.

The availability of financial intelligence for understanding the operations of a territory-controlling group may also be limited. First, most of its economic activity will be confined to the territory it holds and authorities will have limited access to intelligence sources, such as suspicious transaction report filings or other forms of financial transaction data that they would typically rely on for gathering financial intelligence. Captured documents have on occasion provided financial intelligence that can be exploited,[120] and the use of mobile money platforms accessible outside the area of territorial control may open financial intelligence opportunities.[121] Where financial institutions may gather valuable intelligence is in connecting a group with its foreign outposts, such as affiliated OCG-type groups or small cells and lone actors, or identifying financial flows connected with fighters travelling to join or returning from a terrorist group such as ISIL. Second, it will not be possible to use financial intelligence for prosecution or asset freezes and confiscation as long as the suspects and their assets are de facto beyond the reach of law enforcement.

118. Jimmy Gurulé, 'Utilizing Secondary Sanctions to Curtail the Financing of the Islamic State', *Georgetown Journal of International Affairs* (Vol. 18, No. 1, Winter/Spring 2017), pp. 36–42.
119. Jeffrey A Meyer, 'Second Thoughts on Secondary Sanctions', *University of Pennsylvania Journal of International Law* (Vol. 30, No. 3, 2014), p. 905.
120. Yeganeh Torbati and Brett Wolf, 'In Taking Economic War to Islamic State, US Developing New Tools', *Reuters*, 24 November 2015.
121. See, for example, reported use of M-PESA by Al-Shabaab, UN Security Council, 'Letter Dated 1 November 2019 from the Chair of the Security Council Committee Pursuant to Resolution 751 (1992) Concerning Somalia Addressed to the President of the Security Council'.

The primary objectives of CTF measures in relation to a territory-controlling group are therefore to ensure isolation from the financial system beyond its borders and reduce access to resources. This can be achieved by the use of military action and limiting the group's ability to sell resources to finance its operations. For example, tight enforcement of the ban on the sale of Somali charcoal should have restricted Al-Shabaab's revenue raising.[122] In contrast, CTF measures that focus on cutting off a group from the international financial system and limiting the inflow of donations will have only a limited impact on the revenue of an organisation functioning as a quasi-state. It will also restrict access to the sourcing of resources and distributing funds to support affiliates. But, so long as internal sources of funding remain, the group will continue to exist.

As a result of this analysis, military action appears indispensable for defeating a territory-controlling group; in that context, focusing strikes on key nodes of the economic infrastructure may be a valuable strategy. Operations against ISIL are a case in point. According to one former US government official, the best CTF advice the US Treasury had during the height of ISIL's activity was to drop bombs on revenue generating assets such oil wells and tankers, as well as cash storage facilities.[123] This state of affairs is a reflection of the fact that reducing terrorist access to resources – one of the objectives of the CTF regime – need not be achieved through financial means alone.[124]

OCG-Type Groups

A number of terrorist groups display characteristics that set them apart from both territory-controlling groups, and small cells and lone actors. Unlike the former, they do not exercise exclusive control over any geographical area. At the same time, in contrast to small cells and lone actors, they maintain a developed hierarchy and fulfil a wide range of functions, such as carrying out attacks, raising funds, distributing propaganda and providing support to members of the group or their families. In order to do so, such groups tend to acquire substantial material resources.

In recognition of the similarity between the financial modus operandi of this second group and those of organised criminals, this paper refers to these as OCG-type groups and distinguishes between those that operate in an area that the respective government cannot fully and effectively control and those that operate in an area under effective governmental control.

---

122. For further details see UNSCR 2036, OP22.
123. Authors' interview conducted with a former US government official, Washington DC, October 2017.
124. The importance of remembering this, rather than focusing exclusively on the 'follow-the-money' approach, was highlighted by Michael Braun during the hearings in the US House of Representatives in June 2016. See US House of Representatives, The Task Force to Investigate Terrorism Financing, Committee on Financial Services, 'The Enemy in Our Backyard: Examining Terror Funding Streams from South America', 114th Congress, Second Session, 8 June 2016.

In order to pursue their objectives, such as the establishment of a new state or the reorientation of society towards a particular religious dogma, both kinds of OCG-type groups need to employ varied methods for raising finances, often operating discreetly and sometimes across multiple jurisdictions. In contrast to territory-controlling groups that operate devoid of meaningful government presence, the more effective the governmental control is over the area in which these groups operate, the more opportunities there are for law enforcement interventions, thus the more creative and diversified the funding model of this category needs to be.

Fundraising Methods

Criminal Income

Since terrorist financing is commonly treated as a crime, all terrorist income is legally 'criminal'. However, a distinction can be made between income that derives from inherently criminal activities (for example, bank robberies or trafficking in illicit goods) and income that comes from legitimate activities. While the former activities are evidently unlawful and criminal, the latter appear legitimate unless and until a connection with terrorism or organised crime is proven. In practical terms, the distinction matters most in areas where the government is in control and can enforce the rule of law, hence it is of greater relevance when applied to OCG-type groups and small cells and lone actors operating within functioning states than to territory-controlling groups that exploit a lack of government control.

Available evidence documents a panoply of criminal activities that are or can be used by OCG-type groups. For instance, FATF, GABAC (Task Force on Money Laundering in Central Africa) and GIABA (Inter-Governmental Action Group Against Money Laundering in West Africa)[125] list the following sources of terrorist funding in West Africa, most of which constitute criminal activities:[126]

- Confirmed sources of funding:
    - Extortion.
    - Robberies and looting.
    - Cattle/livestock rustling.
    - Donations.
    - Abuse of NPOs.
    - Extortion of businesses/commercial enterprises.
    - Kidnapping for ransom.

- Suspected and potential sources of funding:
    - Trafficking of drugs, weapons and other goods.
    - Smuggling of migrants and trafficking in persons.

125. These are two of FATF's so-called FATF-style regional bodies (FSRBs). They respectively consist of seven and 16 members.
126. FATF, GIABA and GABAC, 'Terrorist Financing in West and Central Africa', p. 11.

- Oil and cigarette smuggling.
- Piracy.
- Cybercrime and fraud.

The list is notable for highlighting the opportunistic and context-specific nature of terrorist financing, such as the engagement of terrorists in cattle-rustling in those areas in West Africa where cattle represent a valuable and relatively easily transportable asset.

Illustrative of the blurred lines between the categorisation of groups, the above list includes tactics similar to those of territory-controlling groups, namely:

- Rent-seeking from businesses.
- Extortion of the population.
- 'Taxation' of trade routes, including those used by criminals.

Drug trafficking appears widespread among terrorist groups across the world as a means of fundraising. For example, Hizbullah[127] has been linked to drug trafficking in South America.[128] And in 2011 the Drug Enforcement Agency's Operation *Titan* led to the identification by the US Treasury of the Lebanese Canadian Bank SAL (LCB) as a financial institution of primary money-laundering concern under Section 311 of the USA PATRIOT Act (2001).[129] According to the US Treasury, Hizbullah derived financial support from the drug-trafficking network allegedly run by Ayman Saied Joumaa, who is reported to have laundered up to $200 million per month via the LCB.[130] As this designation highlights, targeting cross-cutting enablers that facilitate both criminal and terrorist activities can be an effective disruption strategy.[131]

The perceived importance of drug trafficking to Hizbullah's funding model is underlined by the establishment in January 2018 of the Hizbullah Financing and Narcoterrorism Team within the

127. Hizbullah 's military and political wings are considered terrorist organisations by the US, the Netherlands and the UK – however the EU has only designated its military wing.
128. US House of Representatives Committee on Financial Services, the Task Force to Investigate Terrorism Financing, Committee on Financial Services, 'Stopping Terror Finance: Securing the US Financial Sector', p. 14; Matthew Levitt, 'Hezbollah's Criminal Networks: Useful Idiots, Henchmen, and Organized Criminal Facilitators', in Hilary Matfess and Michael Miklaucic (eds), *Beyond Convergence: World Without Order* (Washington, DC: National Defense University, 2016).
129. US Department of the Treasury, 'Treasury Identifies Lebanese Canadian Bank Sal as a "Primary Money Laundering Concern"', 10 February 2011; US House of Representatives, the Task Force to Investigate Terrorism Financing, Committee on Financial Services, 'A Dangerous Nexus: Terrorism, Crime and Corruption'.
130. US Department of the Treasury, 'Treasury Identifies Lebanese Canadian Bank Sal as a "Primary Money Laundering Concern"'.
131. Florence Keen and Anton Moiseienko, 'Much Ado About the Nexus: Why Does the Crime/Terror Nexus Matter?' *RUSI Newsbrief* (Vol. 38, No. 7, 2018).

US Department of Justice.[132] Furthermore, a dedicated provision of US federal criminal law – 21 USC. § 960a[133] – prescribes increased punishment for drug trafficking with knowledge or intent that any of the proceeds will support a terrorist organisation. The first person sentenced under that law was Jose Maria Corredor-Ibague, an international drug trafficker who cooperated with the FARC.[134]

In 2003, a senior official in the DEA reported 'that 14 of the 36 groups designated as foreign terrorist organizations on the U.S. State Department's list are involved in drug trafficking'.[135] For instance, in Peru, the communist insurgent group Sendero Luminoso (Shining Path) allegedly generated $50,000 to $100,000 per month from selling drugs as of 2014, although its military strength was limited and its operations largely confined to one valley.[136]

Depending on the context and their profitability, a range of other crimes may be used by terrorists to raise funds, especially in the case of sophisticated terrorist groups that operate as transnational criminal enterprises. For example, crimes involving Hizbullah operatives include a cigarette-smuggling scheme devised by the Hammoud brothers, Mohamad and Chawki, in the US states of North Carolina and Michigan, which generated $8 million in profits.[137]

The Crime–Terror Nexus

The prospect of criminals and terrorists operating together has been a central concern of the international community for many years. In the aftermath of 9/11, UNSCR 1373[138] noted the close connection between international terrorism and transnational organised crime, listing threats including illicit drugs, money laundering and illegal arms trafficking as a source of terrorist financing. In 2014, UNSCR 2195 listed additional threats by which terrorists can profit, including the trafficking of arms, persons, natural resources, wildlife, charcoal and oil; in 2018, the Global Counter Terrorism Forum published The Hague Good Practices on the Nexus Between

132. US Department of Justice, 'Attorney General Sessions Announces Hezbollah Financing and Narcoterrorism Team', 18-30, press release, 11 January 2018, <https://www.justice.gov/opa/pr/attorney-general-sessions-announces-hezbollah-financing-and-narcoterrorism-team>, accessed 31 December 2019.
133. 21 USC § 960a. 'Foreign Terrorist Organizations, Terrorist Persons and Groups'.
134. US Department of Justice, 'High-Level Colombian Drug Trafficker Sentenced to 194 Months in Prison', 13-1029, press release, 16 September 2013, <https://www.justice.gov/opa/pr/high-level-colombian-drug-trafficker-sentenced-194-months-prison>, accessed 31 December 2019.
135. Yvon Dandurand and Vivienne Chin, 'Links Between Terrorism and Other Forms of Crime', report submitted to Foreign Affairs Canada and the UNODC, December 2004, p. 12.
136. US House of Representatives Committee on Financial Services, the Task Force to Investigate Terrorism Financing, 'Stopping Terror Finance: Securing the U.S. Financial Sector'.
137. US vs. Mohamad Youssef Hammoud, US Court of Appeals for the Fourth Circuit, 381 F.3d 316, 2 August 2004.
138. UNSCR 1373.

Transnational Organized Crime and Terrorism;[139] and in 2019, UNSCR 2482 reiterated the calls on member states to enhance coordination efforts against the links between international terrorism and organised crime.

Box 2: The Hague Good Practices on the Nexus Between Transnational Organized Crime and Terrorism

The Hague Good Practices are based on discussions with experts within government, international, national and regional organisations, academia and other relevant stakeholders during four regional meetings held in 2017 and 2018 in Algiers, Tirana, Singapore[i] and Nairobi focusing respectively on West Africa and the Sahel, the Balkans, Southeast and South Asia, and the Horn of Africa and East Africa.

The document outlined four key sections where urgent action could be taken to disrupt the nexus: legal considerations; research and information sharing; local engagement; and capacity building and law enforcement. As regards CTF, three Good Practices from the document are pertinent:

Good Practice 11: Encourage the use of information from peripheral sources and new methods of information collection, including financial intelligence which can be exploited to target illicit financial flows. Financial intelligence is recognised by this recommendation as a significant information source, particularly in relation to the organised crime/terror nexus given the extent to which – to varying degrees – both organised crime and terrorist groups rely on funding to conduct their activities.[ii]

Good Practice 12: Support the further development of private and public sector partnerships to assist in combating the nexus, including, but not limited to, the field of financial investigation.[ii]

This reflects the wealth of information private sector companies have, and thus the benefit in partnering with them when it comes to understanding the intersection between crime and terrorism.

Good Practice 21: Increase financial investigative capacities by training relevant agencies to carry out financial investigations to deprive transnational organised crime and terrorist groups of the various resources used to pursue their criminal activities. The private sector should also be leveraged to support the effectiveness of financial investigation activity.[iv]

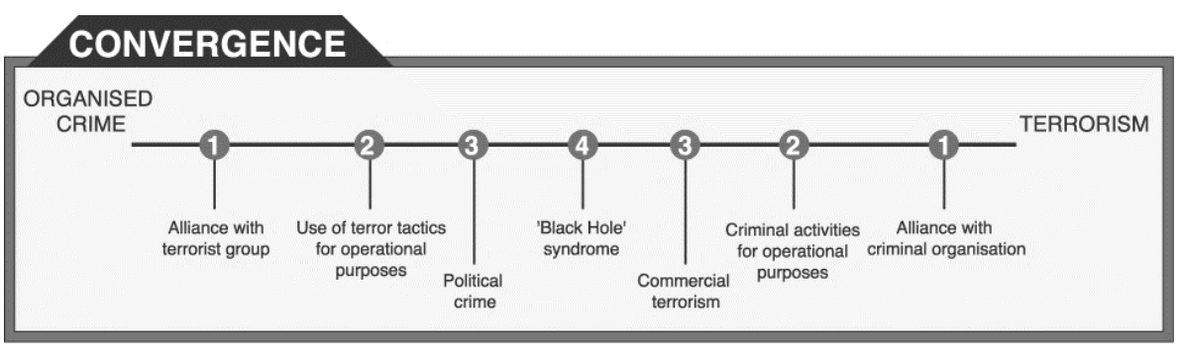
i. Florence Keen gave expert evidence on the nexus at this meeting in Singapore in March 2018.
ii. Global Counter Terrorism Forum, 'Policy Toolkit on The Hague Good Practices on the Nexus Between Trasnational Organized Crime and Terrorism', 2019, p. 26.
iii. *Ibid*., p. 28.
iv. *Ibid*., p. 46.

139. Global Counter Terrorism Forum, 'Policy Toolkit on The Hague Good Practices on the Nexus Between Transnational Organized Crime and Terrorism', 2019.

Of note, UNSCR 2482 emphasises Good Practice 20,[140] highlighting the links between terrorism and petty crime and the potential for recruitment and radicalisation of criminals in the prison system.[141] Understanding where connections between the criminals and terrorists exist is arguably beneficial for those tasked with detecting and disrupting terrorist finance, as law enforcement actors can shape their interventions more effectively to disrupt both.

The challenge for policymakers and practitioners working in the CTF space is that 'nexus' can take a number of different meanings – from criminals and terrorists operating in unison, to simply the use of criminal tactics by terrorist actors. The academic debate reveals a wide divergence in interpretation. The crime–terror nexus first achieved prominence in academic circles via the work of Tamara Makarenko in 2004, who conceived the nexus as a 'continuum' of different forms of engagement.[142] Criminal and terrorist organisations were seen to emulate one another – adapting to each other's successes and failures, through 'alliances', suggesting a degree of cooperation around shared skills such as money laundering or smuggling routes; 'operational motivations', in which terrorists acquire criminal skills to achieve their objectives, or vice versa; and 'convergence', in which criminal and terrorist organisations become a fused entity, displaying the characteristics of terrorist and criminal simultaneously. Regardless of where a group sits on the continuum, Makarenko suggests that the law enforcement response should focus on the criminal activity itself, and in particular on limiting a group's access to finance.

Figure 1: The Crime–Terror Continuum



Source: Tamara Makarenko, 'The Crime–Terror Continuum: Tracing the Interplay Between Transnational Organised Crime and Terrorism', Global Crime (Vol. 6, No. 1, February 2004), pp. 129–45.

It has conversely been argued that the concept of a nexus has been exaggerated and is based upon a confirmation bias by which analysts attempting to look for a relationship will invariably find one.[143] While cooperation may exist when terrorists and criminals share a geographic space,

140. *Ibid*., p. 44.
141. UNSCR 2482, 19 July 2019.
142. Tamara Makarenko, 'The Crime–Terror Continuum: Tracing the Interplay Between Transnational Organised Crime and Terrorism', *Global Crime* (Vol. 6, No. 1, February 2004), pp. 129–45.
143. Phil Williams, 'The Organised Crime and Terrorist Nexus, Overhyping the Relationship,' *Stratfor*, 20 April 2018.

such as the use of professional enablers, this represents convenience rather than evidence of a formal nexus. Criminals are by their nature opportunistic. Those that offer services – dubbed 'crime as a service' by Europol – are likely to be agnostic as to from whom they earn an income.

One might reasonably ask why an OCG would wish to operate in any sort of formal arrangement with a terrorist group, as this is likely to draw unwelcome attention from law enforcement and security authorities to the criminals' activities, unnecessarily increasing operational risks and attendant penalties. Furthermore, the false belief in a crime–terror nexus may result in governments devoting security-related resources inappropriately. Al-Shabaab's supposed, but unevidenced, engagement in illegal wildlife trade is a case in point.[144]

By contrast, there are numerous examples of terrorist organisations *adopting* criminal tactics, rather than *collaborating* with OCGs. The IRA's activities in the 1980s and 1990s revealed a high level of criminal activity and related financial sophistication, generating income through money-laundering schemes, the smuggling of livestock, tobacco, the pirating of video and audio tapes and computer games.[145] According to Northern Irish law enforcement, following the Good Friday Agreement, there has been a significant increase in organised crime activity as the criminal skills acquired by terrorists to fund their political violence – such as 25 years of money-laundering experience – can be put to new use. They estimate that around 60% of OCGs in the country have paramilitary links.[146]

Tobacco-smuggling has remained a key source of finance for Northern Ireland and Republic of Ireland paramilitaries, with cigarettes reportedly being shipped from factories in Asia, Eastern Europe and the Middle East, then smuggled into mainland UK where their sale has allowed IRA hard liners to amass considerable sums of money.[147] With the threat from Northern Ireland-related terrorism (NIRT) in 2017 assessed as 'severe' in Northern Ireland and 'substantial' on the mainland, income through cigarette smuggling, fuel laundering, extortion and robbery[148] require continued law enforcement resources and intervention. Law enforcement interviewed for this paper confirmed that fuel excise fraud was a major concern at present.[149]

An example of terrorist groups collaborating in a more formal way with OCGs can be seen in the Afghanistan–Pakistan region where local conditions have provided opportunities for both criminals and terrorists to carry out illicit activities due to a combination of corruption, porous

144. Tom Maguire and Cathy Haenlein, 'An Illusion of Complicity: Terrorism and the Illegal Ivory Trade in East Africa', RUSI Occasional Paper (September 2015).
145. John Horgan and Max Taylor, 'Playing the "Green Card" – Financing the Provisional IRA: Part 1', *Terrorism and Political Violence* (Vol. 15, No. 2, 2003).
146. Authors' interview with Northern Irish law enforcement agency, Belfast, March 2018.
147. George Arbuthnott and John Mooney, 'The Smoking Gun: How Cigarettes Became the IRA's New Weapon', *The Times*, 15 February 2015.
148. Home Office and HM Treasury, *National Risk Assessment of Money Laundering and Terrorist Financing 2017* (London: The Stationery Office, 2017).
149. Authors' interview with Northern Irish law enforcement agency, Belfast, March 2018.

borders and weak rule of law.[150] In 2019, the UN noted strong ties between the Taliban and OCGs in a number of Afghan provinces, describing a '50/50 partnership' that has allowed the Taliban to profit from revenues generated from heroin, hashish, pine nuts and the extortion of local businesses.[151]

Yet, while some question the concept of a crime–terror nexus, the concept may have a role to play where it enables the identification of opportunities to dismantle both terrorist and criminal operations via targeting nodes that support both. This could include an unwitting or agnostic money-service business being abused by both criminals and terrorists.

Providing services on behalf of terrorists may also be purposeful. The Khanani Money Laundering Organisation (MLO) laundered illicit proceeds for OCGs, drug-trafficking organisations and terrorist groups throughout the world. Altaf Khanani, head of the Khanani MLO and Al Zarooni Exchange, is known to have been involved in the movement of funds for the Taliban, as well as having relationships with South Asian terrorist group Lashkar-e-Taiba, Dawood Ibrahim – India's most-wanted underworld figure with a $25-million reward on his head – Al-Qa'ida and Pakistani-Kashmiri jihadists Jaish-e-Mohammed.[152] In 2015, the US Department of the Treasury's Office of Foreign Assets Control designated the Khanani MLO as a transnational criminal organisation, pursuant to Executive Order 13581.[153]

As the recently passed UNSCR 2482 notes, member states and their law enforcement agencies need to enhance their knowledge of 'the nature and scope of the linkages that may exist between terrorism and organized crime'.[154] Simply asserting that a crime–terror nexus exists is not sufficient. As with all forms of terrorist financing, a clear understanding of the risk and the means by which financing is raised and resources are procured is key to determining the appropriate CTF strategy.

Lawful Income and Investments

Since OCG-type groups often need to operate within government-controlled areas that benefit from functioning law enforcement, they also seek to rely on lawful sources of funds that can only be constricted by the government if the purpose to which they are put becomes known. The two major sources of such income are running legitimate businesses and soliciting donations.

150. Reitano, Clarke and Adal, 'Examining the Nexus Between Organised Crime and Terrorism and its Implications for EU Programming'.
151. Djani, 'Letter Dated 10 June 2019 from the Chair of the Security Council Committee Established Pursuant to Resolution 1988 (2011) Addressed to the President of the Security Council'.
152. FATF, 'Professional Money Laundering', July 2019.
153. US Department of the Treasury, 'Treasury Sanctions the Khanani Money Laundering Organization', 12 November 2015.
154. UNSCR 2482, 19 July 2019, S/RES/2482 (2019).

For instance, the IRA were known to gain 'income from control over taxi cabs, gaming machines and donations'.[155] Similarly, Hizbullah is said to operate a network of businesses across the world, in particular in Latin America and in Africa, which engages with, among other things, 'international trade as well as real estate'.[156]

The use of legitimate business allows terrorists to accomplish several objectives. First, it may provide a steady source of revenue that is less prone to law enforcement intervention until the business's terrorist connections come to light. Second, it may serve as a vehicle for investing and storing funds, thereby addressing one of the challenges that financially successful terrorist groups may face. Third, international business operations can offer a convenient pretext for the cross-border movement of funds. For example, Hizbullah has employed trade-based money-laundering schemes to move money to Lebanon via the export of used cars from the US to West Africa, from where the sale proceeds would be repatriated to Lebanon through bulk cash deposits.[157]

CTF Responses

A range of terrorist groups have demonstrated considerable financial prowess in raising funds via a variety of different criminal methods. While there is some limited evidence of a 'nexus' between terrorists and organised crime, more often the former adopt criminal methods to support their fundraising. For this reason, the authors have dubbed them OCG-type terrorist groups. Where there is crime–terror interaction, it is most likely to be a marriage of convenience rather than any sort of formal alliance.

OCG-type groups operating in governed territories are susceptible to the same kinds of law enforcement interventions as 'non-terrorist' OCGs, including criminal prosecution, asset confiscation, sanctions designations or deportations of individual members. In this context, financial intelligence can play a useful role in identifying the extent of terrorists' (financial) networks and their affiliates, detect assets that may be liable to confiscation, and build up an evidential case that can be used in court.[158]

In contrast, those OCG-type groups that carry out their activities in contested areas beyond the de facto reach of law enforcement have to be tackled in a manner similar to that used

155. Levi, 'Combating the Financing of Terrorism', pp. 650, 662.
156. US Department of the Treasury, 'Treasury Targets Hizballah Financial Network', 9 December 2010. See also *The Sentry*, 'The Terrorists' Treasury: How A Bank Linked to Congo's President Enabled Hezbollah Financiers to Bust US Sanctions', October 2017.
157. US House of Representatives Committee on Financial Services, the Task Force to Investigate Terrorism Financing, Committee on Financial Services, 'Stopping Terror Finance', pp. 4, 11.
158. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: FATF Recommendations', Interpretive Note to Recommendation 30, updated October 2018, p. 98.

against territory-controlling terrorist groups, with a heavier emphasis on military operations by government forces.

Lone Actors and Small Cells

For many jurisdictions, particularly in the West, the most visible terrorist risk today comes from small cells and lone actors, who may be inspired to commit attacks after a rapid radicalisation period, often following exposure to extremist content online.[159] As Nick Rasmussen, the former director of the US National Counterterrorism Center, noted in 2015: 'The "flash to bang" ratio in plotting of this sort [of attack] is much quicker and allows for much less time for traditional law enforcement and intelligence tools to disrupt or mitigate potential plots'.[160] According to FATF, in terrorist plots involving lone actors and small cells, it is likely that the costs associated with the lethal component of the plot (for example, obtaining assault rifles and explosives or funding pre-operational, out-of-country travel for training) represents the most expensive part of what may actually be a low-cost attack.[161] Tim Krieger and Daniel Meierrieks note that 'sleeper cells and "lone wolf" terrorist activity, which is only loosely connected to the over-arching structure of a terror network, require fewer and smaller financial transfers [if at all], which can be less easily detected by money laundering prosecutors'.[162] This form of terrorist attack was not under consideration when the global architecture was formed in the aftermath of the 9/11 attacks and requires a new form of thinking that is most often not captured by existing CTF approaches.

Lone actors and small cells may operate in contested or government-controlled areas. However, unlike the groups mentioned thus far (territory-controlling and OCG-style), they operate without substantial resources and have no need for any meaningful form of organisational structure or hierarchy. The speed and ease with which small cells and individuals can manufacture acts of violence have been well recognised and actively encouraged by larger terrorist organisations, forming part of their global strategies. In May 2016, Abu Muhammad Al-Adnani, former official spokesperson of the Islamic State, stated: 'The smallest action you do in their heartland is better and more enduring to us than what you would [do] if you were with us. If one of you hoped to reach the ISIL, we wish we were in your place to punish the Crusaders day and night'.[163]

159. Extensive academic research has been conducted on the definition and motivation of lone actors and small cells. See, for example, Clare Ellis et al., 'Lone-Actor Terrorism: Final Report', *RUSI Occasional Papers* (April 2016), and supporting data and research available at <https://rusi.org/projects/lone-actor-terrorism>, accessed 22 August 2019.
160. Paul Cruickshank, 'A View from the CT Foxhole: An Interview with Nick Rasmussen, Director, NTCT', *CTC Sentinel* (Vol. 8, No. 9, 2015).
161. FATF, 'Emerging Terrorist Finance Risks', October 2015.
162. Tim Krieger and Daniel Meierrieks, 'Terrorist Financing and Money Laundering', University of Paderborn, Germany, June 2011.
163. Maher Chmaytelli, Stephen Kalin and Ali Abdelaty, 'Islamic State Calls for Attacks on the West During Ramadan in Audio Message', *Reuters*, 22 May 2016.

Indeed, the deaths of a handful of people from a Western country at the hands of a home-grown terrorist may be as strategically important to a terrorist organisation as the deaths of hundreds of people within a conflict zone.

There has been limited study of the financing of small-cell and lone-actor terrorism, primarily because this form of actor requires minimal finance to commit a low-tech attack, for example, using a knife or driving a van into a crowded public space.[164] Often, the individual or small cell may already have access to these tools, precluding any need for funds; or the funds needed are unlikely to raise suspicion. This makes the job of financial institutions and law enforcement extremely challenging, in what one US law enforcement officer described as searching for 'needles amongst needles'.[165] FATF has noted that:

> In contrast to large terrorist organisations, small cells and individual terrorists face only minor financial needs since costs of terrorist attacks are often small. As such, lone actors and small cell terrorist networks have a much smaller funding requirement given that they do not control territory, field conventional militias, engage in recruitment or propaganda operations, operate checkpoints or deliver social services.[166]

In 2017, a RUSI *Occasional Paper* studied the financial behaviour behind a sample of lone-actor and small-cell terrorist plots in the UK, France and Australia between 2000 and 2014.[167] It found that the plotters and attackers were often able to make use of their own resources, providing limited financial indicators prior to the execution of an attack. Moreover, the financial patterns of lone-actor and small-cell operators were generally indistinguishable from legitimate financial activity. For example, the murderers of Lee Rigby in 2013, Michael Adebolajo and Michael Adebowale, were reported to have purchased a knife, which would be unlikely to cost more than £20–30.[168] The ability for law enforcement to detect this type of pre-attack financial activity is vanishingly small.

A further academic study in 2017 sampled 55 lone-actor cases and found that only 13% of these took steps to secure extra finances that went above their existing sources of income in attack preparation stages. This, the authors argue, points to the unsophisticated and inexpensive nature of lone-actor attacks.[169] Faced with such a limited financial picture, the utility of focusing on identifying and restricting funding must be questioned. In such cases, it is likely financial intelligence can play a more central role in connecting actors and mapping networks, providing

164. A notable study of this issue is provided by Oftedal, 'The Financing of Jihadi Terrorist Cells in Europe'.
165. Authors' interview with US law enforcement officer, Washington, DC, October 2017.
166. FATF, 'Emerging Terrorist Financing Risks'.
167. Tom Keatinge and Florence Keen, 'Lone-Actor and Small Cell Terrorist Attacks: A New Front in Counter-Terrorist Finance?', *RUSI Occasional Papers* (January 2017).
168. *BBC News*, 'Woolwich: How Did Michael Adebolajo Become a Killer?', 19 December 2013.
169. Bart Willem Schuurman et al., 'Lone Actor Terrorist Attack Planning and Preparation: A Data Driven Analysis', *Journal of Forensic Sciences* (Vol. 63, No. 1, 2017), pp. 1191–1200.

indicators of threat activities and – where an attack is disrupted or successfully executed – contributing to investigations that may, in turn, provide leads that identify and disrupt potential future terrorist attacks.

Fundraising Methods

As described above, the funds required for lone-actor and small-cell actors are likely to be minimal. Nonetheless, all terrorist actors require some level of finance to sustain their living costs, and/or manufacture an attack. The typical generation of income by small cells and lone actors can be divided as follows:

- Income generated from legitimate activity, for example:
    - Salary from legitimate business.
    - Welfare payments.
    - Student loans.
    - Payday loans.

- Income generated from low-level crime, for example:
    - Fraud.
    - Counterfeiting.
    - Drug dealing.
    - Online crime (for example, via the dark web).

Legitimate Activity

Terrorist fundraising through legitimate activity appears across multiple terrorist actors described in this paper, and is not unique to lone actors and small cells – however, it is arguably the most important method for this group. Why commit a criminal offence and risk being detected and disrupted by law enforcement, when you can use the resources that are already at your disposal?

There are a number of cases that highlight the use of an individual's own, a spouse's or relative's salary to support an attack. For example, the investigation and disruption of a plot by Mohammed Rehman and Sana Ahmed Khan, a British couple who had planned attacks on the 10th anniversary of the July 2005 London transport bombings, revealed the use of Khan's own salary as a teaching assistant, in addition to payday loans.[170] In the case of the 2015 San Bernardino attack in California, perpetrated by married couple Syed Rizwan Farook and Tashfeen Malik, the former was found to have borrowed approximately $28,500 from online

170. Tom Whitehead and David Barrett, 'Middle Class Daughter of Magistrate Who Turned to Suicide Bomb Plotter', *The Telegraph*, 20 December 2015; Owen Bowcott, 'Couple Found Guilty of 7/7 Anniversary London Bomb Plot', *The Guardian*, 29 December 2015.

lender 'Prosper Marketplace' prior to the attack in December 2015.[171] It is suspected that this money may have financed Farook's ammunition and shooting practice at local gun ranges.[172]

Benefit and welfare payments have also been documented as sources of terrorist financing. For example, Mohamed Abrini, known as the 'man in the hat' involved in the Brussels airport bombings of 2016, received £3,000 in cash in July 2015 from the account of a Belgian national, Anouar Haddouchi. The latter was still receiving benefit payments from the UK government into an account registered in Britain, despite having left the country to fight in Syria in 2014.[173] In Sweden, the foreign terrorist fighter, Michael Skramo, was paid the equivalent of over $5,000 for more than eight months after leaving with his wife and four children to fight in Syria.[174] This systemic failing was repeated on numerous occasions across Europe during recent years, where state benefits have been co-opted for terrorist-related activity.[175]

Criminal Methods

Another consideration is the connection between lone-actor/small-cell terrorism and petty crime, as referenced in the earlier discussion on the crime–terror nexus. This connection has come into particular focus in recent years in relation to low-level criminals from the Muslim community who have moved from a criminal lifestyle to conducting terrorist attacks. There is evidence that these individuals have been encouraged to use the criminal financing skills they have acquired as a means of waging jihad. It has been argued that the crime–terror nexus in Europe is represented not by the convergence of criminal and terrorist groups, but by social networks, with recruits to criminality and terrorism often drawn from the same pools.[176] For example, the cell that attacked the *Charlie Hebdo* offices in Paris, January 2015 had been known to engage in the trade of counterfeit sportswear ahead of committing the attacks.[177] Taking France as an example, of 78 convicted jihadist terrorists between 2015 and 2016, 48.7% were found to have a record of prior

171. James Rufus Koren and Jim Puzzanghera, 'Loan to San Bernardino Shooter Draws Scrutiny to Online Lending Industry', *Los Angeles Times*, 11 December 2015.
172. Matthew Levitt, 'Low Cost, High Impact: Combatting the Financing of Lone-Wolf and Small-Scale Terrorist Attacks', Testimony Submitted to the Terrorism and Illicit Finance Subcommittee, House Financial Services Committee, 6 September 2017.
173. Mark White, 'Pair Convicted After Giving Money to Brussels Bomb Suspect', *Sky News*, 6 December 2016.
174. Kim Hjelmgaard, 'European Welfare Benefits Help Fund ISIL Fighters', *USA Today*, 23 February 2017.
175. Mark Maremont and Valentina Pop, 'Terrorist Suspects in Europe Got Welfare Benefits While Plotting Attacks', *Wall Street Journal*, 4 August 2016.
176. Rajan Basra, Peter R Neumann and Claudia Brunner, 'Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus', International Centre for the Study of Radicalisation and Political Violence, King's College London, 2016.
177. Maysa Razavi, 'Untangling the Worldwide Web of Counterfeiting,' World Trademark Review, 24 May 2018.

arrests for petty crimes, including theft, robbery and selling stolen goods. The same report notes that most of these were 'one-time' offences, with very few career criminals within the data.[178]

It is often difficult to determine the extent to which criminal finances themselves are used to fund this style of terrorist attack. For example, the case of Tarik Hassane and Suhaib Majeed, who in 2016 planned a drive-by shooting in the Shepherd's Bush area of West London, but were disrupted,[179] revealed a PayPal fraud scheme in the attack-planning phase. However, there was no indication at the time the fraud was committed that this money would be spent on the intended plot. Nevertheless, it is important that the CTF community develops its understanding of the links between low-level crime and lone-actor and small-cell terrorism. This may help to identify actors involved in criminal activity who, as noted above, may be vulnerable to radicalisation and warrant greater attention of and connectivity between local community groups and police forces.

Movement of Funds

While small cells and lone actors may gather inspiration from, or be directed by, larger terrorist groups such as ISIL, most often, they lack financial connections to a wider group, relying on their own income or petty crime to fund their activities. Between themselves, however, individual members of a cell will almost certainly be connected.

Financial transactions may also reveal a lone actor's support of an established group, even if the individual is largely unconnected. For example, Brenton Tarrant, the accused murderer of 51 people in Christchurch, New Zealand in March 2019, was revealed to have made a significant donation of funds to the Identitarian Movement of Austria after electronic devices were seized from the home of its leader, Martin Sellner.[180] While there is no indication that this transfer funded nefarious activity in Austria, this financial movement reveals the existence of an ideological connection, and perhaps an insight into where Tarrant drew (some of) his inspiration from.

178. Pierre Colomina, Olivier de France and Damien Saverot, 'From Criminals to Terrorist and Back: The In-Betweeners? Links Between Crime and Terror in France', GLOBSEC Defence & Security Programme, Quarterly Report, 2019.
179. Emily Pennink, '"Drive-by Jihad" Plotters Tarik Hassane and Suhaib Majeedi Jailed for Life', I*ndependent*, 23 April 2016.
180. Emma Reynolds, 'Inside the Dark, Neo-Nazi Movement Linked to Christchurch Terrorist', *News. Com.Au*, 27 March 2019.

Box 3: The Extreme Right Wing

In many parts of Europe, North America and other Western countries, the threat of violence from the extreme right wing is on the rise. From the murder of Labour MP Jo Cox in the UK in 2016, to the shooting of Muslim worshippers in Christchurch, New Zealand, in 2019, it is a threat that primarily emanates from lone actors and small cells. However, more structured groups such as the UK proscribed organisation National Action are on the increase.

While extreme right-wing groups have employed notable fundraising techniques, such as hosting music festivals, the fundraising methods of individuals (the most deadly risk in recent years) do not yet look fundamentally different from other lone actors and small cells that have been studied.[i] This is because the funds required for this form of attack are also minimal, often simply requiring a van or a knife. For example, Pavlo Lapshyn, a Ukrainian student who murdered Mohammed Saleem in Birmingham in 2013, used a knife that would have either been his own, or would have cost no more than £20.[ii]

Financial leads may, however, play a valuable role in investigations: Cox's killer was found to have purchased manuals on the construction of homemade pistols, issues of the National Alliance journal, and a rare surviving copy of *Ich Kämpfe*, which was handed out to Nazi Party members in 1943.[iii] While on their own this may not have indicated anything unusual, together they paint a picture of an individual who may be inclined towards extreme right-wing views.

At present, while coordination between extreme right-wing actors appears limited to drawing on or sharing ideology and grievances, evidence of international connectivity is increasing. For example, funds have been raised in the US to support the UK legal fees of Tommy Robinson.[iv] Furthermore, evidence is emerging of places such as Ukraine, home of the Azov Battalion, acting as 'hotspots' that attract extreme right-wing travellers.[v]

i. See Tom Keatinge, Florence Keen and Kayla Izenman, 'Fundraising for Right-Wing and Extremist Movements: How They Raise Funds and How to Counter It', *RUSI Journal* (Vol. 164, No. 2, 2019),
ii. *BBC News*, 'Mosque Bomber Pavlo Lapshyn Given Life for Murder', 25 October 2013.
iii. Ian Cobain, Nazia Parveen and Mathew Taylor, 'The Slow-Burning Hatred that Led Thomas Mair to Murder Jo Cox', *The Guardian*, 23 November 2016.
iv. Josh Halliday, Lois Beckett and Caelainn Barr, 'Revealed: The Hidden Global Network Behind Tommy Robinson', *The Guardian*, 7 December 2018.
v. Tim Hume, 'Far-Right Extremists Have Been Using Ukraine's War as a Training Ground. They're Returning Home', *Vice*, 31 July 2019; Kacper Rekawek, '"It Ain't Over 'til It's Over": Extreme Right-Wing Foreign Fighters in Ukraine', Counter Extremism Project, 23 September 2019.

CTF Responses

Although lone-actor and small-cell terrorism is low- or no-cost, the impact such attacks can have – particularly in Western countries – has made combating them a priority for global policymakers. Initiatives to secure public spaces from vehicle attacks have been rapidly instigated,[181] information-sharing initiatives have been accelerated[182] and CTF has remained a key element of the work undertaken by government authorities to combat this threat.[183] As one senior UK CTF law enforcement officer remarked, the majority of his team's energy and resources are focused on small-cell and lone-actor risks, despite the ongoing risks posed by larger organisations.[184]

What is clear is that the CTF regime, as it was originally conceived to disrupt established and structured terrorist organisations, is ill-suited to the threat from lone actors and small cells. The finances are small and often from legitimate sources. Even if they are a result of criminal activity, they remain relatively indistinguishable from everyday activity, not passing any threshold that would appear suspicious to a bank, money-service business or other reporting entity. Moreover, if there is a financial footprint, there is no guarantee that this will be within the regulated financial system.

That is not to say that a focus on financing is not of value in this context. Indeed, if CTF is prioritised as the use of finance as an intelligence tool that should be integrated into broader counterterrorism efforts, a rich source of information may be revealed. The financial behaviour of a terrorist actor can expose important connections that identify accomplices or links to a wider group. The ability to understand the existence (or lack) of networks is critically important in the aftermath of an attack as the investigation of a recent attack may lead to opportunities to foil less well-advanced plans.

181. See, for example, European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan to Support the Protection of Public Spaces', COM (2017) 612 final, 17 October 2017.
182. See, for example, Council of the European Union, 'Improving Security Through Information Sharing: Council Agrees Negotiating Mandate on Interoperability', press release, 14 June 2018, <https://www.consilium.europa.eu/en/press/press-releases/2018/06/14/improving-security-through-information-sharing-council-agrees-negotiating-mandate-on-interoperability/>, accessed 23 August 2019.
183. See, for example, Egmont Group of Financial Intelligence Units, 'Public Summary: Counter Terrorist Financing Project Lone Actors and Small Cells', Information Exchange Working Group, July 2019.
184. Authors' interview with senior UK counterterrorism policing officer, London, September 2017.

Recommendations

Ensure that CTF measures are risk-based and align with achievable objectives, including the identification and disruption of:

- The resourcing of terrorist organisations.
- The financing of specific terrorist acts.
- Terrorist activity, by using financial intelligence proactively and reactively.

As this chapter demonstrates, different groups of terrorist actors will employ varied financing methods; the result is that the response of LEAs, security services and the private sector will also need to vary. Table 1 summarises the financing modi operandi of the three categories of terrorist actor featured in this chapter, and the potential related responses.

Table 1: Selected Terrorist Groups, Their Typical Funding Methods and Potential Responses

	Territory-Controlling Groups	OCG-Type Groups	Small Cells and Lone Actors
Operational Characteristics	Control territory.	Operate in a contested area or a government-controlled area.	Operate in a contested area or a government-controlled area.
Funding Requirement	Require resources to maintain military capability; develop promotional material/run media campaigns; provide services to population under its control.	Require resources to maintain activities; manage network; promote cause; run and expand business activities.	Can operate without substantial resources, often relying on legitimate sources of funds. May also be involved in forms of (low-level) criminality.
Structure of Group	Structured responsibilities and hierarchy. Likely to include dedicated financial ministry.	Structured and hierarchical with dedicated and expert financial controllers.	Rarely networked or connected formally to a particular group; more likely to be inspired on/offline or self-radicalised.
Objectives	Fulfil a wide range of functions to achieve one or more political objectives.	Fulfil a wide range of functions to achieve one or more political objectives.	Focus on narrow objective of committing attacks.

	Territory-Controlling Groups	OCG-Type Groups	Small Cells and Lone Actors
Fundraising Methods	Internally derived income such as commodities, natural resources, tax, extortion, kidnap-for-ransom. Some external support may be provided, for example from diaspora donations. State sponsorship is less relevant for these groups.	Criminal methods: illicit trade including drugs/arms/human smuggling, kidnap-for-ransom, embezzlement, extortion of population, rent-seeking from businesses, abuse of NPOs, formal banks and use of money-laundering schemes. Legitimate business may also be operated to generate profits to support terrorist activities. State sponsorship can be material for these groups.	Income generated from legitimate activity: salary from legitimate business or welfare payments; student/pay day loans; or low-level crime, such as fraud, counterfeiting, drug dealing, online crime (Dark Web).
Responses	Isolate the market by ensuring neighbouring countries are engaged in a robust response to the terrorist-financing risks emanating from terrorist-controlled territory, and implement UN and FATF-related CTF requirements. Take back control of territory to deprive group of resources via military action.	Law enforcement intervention including financial methods – anti-money-laundering strategies, use of sanctions and asset freezes and confiscations – and non-financial methods (proscriptions and arrests/prosecutions). Use financial intelligence to develop understanding of network of actors and supporters, including those outside immediate area of terrorist group operations (may be key sympathetic financial facilitators or providers of 'crime as a service').	Intelligence-led/network analysis using financial information, social media analysis and other data points to understand individual activity pre- and post-attack and develop network understanding.

While the classification that was created at the beginning of this chapter between territory controlling and OCG-type groups and lone actors and small cells is necessarily simplistic, this table highlights that some CTF measures are particularly relevant – or, conversely, entirely irrelevant – to certain types of terrorist threat, thus emphasising the importance of applying greater scrutiny to terrorist actor forms and funding methods to devise targeted, risk-based CTF responses.

For instance, governments that face a high risk of small-cell/lone-actor terrorism should consider maximising the use of financial intelligence and tightening controls on the purchase of high-risk products, such as chemicals, or engaging with private sector actors such as vehicle-hire, big-box storage or home-improvement companies. Governments should thus prioritise CTF measures

that are relevant to the terrorist risk they face or the threat they may facilitate via financial activity – such as fundraising by an OCG-type group – within their borders.

Promote collaboration between counterterrorism and law enforcement officials:

- Target professional enablers providing 'crime as a service'.
- Ensure links between crime and terrorist activity are investigated and exploited.
- Implement Hague Good Practices on addressing the nexus between transnational organised crime and terrorism.

Depending on the geography and opportunity, it is clear that terrorists will seek to make use of organised crime tactics to raise funds and further their goals. Evidence of formal partnerships between organised crime and terrorist groups remains limited. Opportunistic partnerships may be formed, but more often, terrorist groups are likely to co-opt the skills and methods of OCGs. Where the notion of a nexus may be useful is through the targeting of professional enablers providing 'crime as a service', such as money-service businesses that are agnostic as to with whom they do business. LEAs must seek to understand where the worlds of organised crime and terrorism overlap, using financial intelligence as a means to support these investigations. This includes developing a greater understanding of the links between low-level crime and lone-actor and small-cell terrorism to identify individuals who may be vulnerable to radicalisation.

Responsible discussion of evidence; avoid inflating terrorist-financing risks

Policy statements by international organisations that highlight a given terrorist-financing modi operandi (for example, references to antiquities trafficking in UNSCRs or unevidenced statements related to the role of the illegal wildlife trade in terrorist financing) can imply that it is more widespread than another modus operandi and thus lead to the misallocation of resources and ineffective strategy. Such statements should be based on a robust assessment of evidence and avoid sensationalisation.

Study the experience of tackling similar terrorist and related financing risks across geographies and time

Although the current CTF regime is associated with the global response to the 9/11 attacks, government efforts to combat terrorism financing have occurred for decades. As illustrated in this chapter, while fundraising methods themselves may alter, the end goal remains much the same. Successful disruption tactics from history (for example, against the PIRA, Hizbullah and ETA) should be recalled and integrated into modern-day strategies where applicable.

Research conducted for this paper reveals that the global CTF memory is, however, poor. In what one academic described as 'responding to the politics of the latest outrage',[185] countries are well versed in grouping together against shared threats. The global response to ISIL typified

185. Authors' interview with UK financial crime academic, London, December 2017.

this, as jurisdictions coalesced against a shared enemy under the Counter-ISIL Finance Group (CIFG).[186] Now that ISIL has been substantially ousted from the territory it controlled, one might question where this institutional knowledge gathered over the past five years will go. As a territory-controlling group, ISIL's methods are neither new nor unique.

Few countries other than the US have the resources to maintain a standing response to terrorist financing that goes beyond that offered by law enforcement and security services. For example, the experience accrued by the UK's Ministry of Defence in targeting Taliban financing in Afghanistan evaporated when that campaign wound down and had to be relearned in the face of the rise of ISIL. It would thus make ample sense to retain the learnings on success and failure of the first phase of the campaign against ISIL financing and ensure that the international community remains 'battle-ready' to respond to future, similar terrorist-financing risks; and that the learning from engaging with ISIL is applied to other territory-controlling groups, such as Al-Shabaab.[187]

Improve understanding of how groups move funds internationally

International transfers should represent a moment of particular vulnerability for terrorists' funds. Yet, the understanding of the ways in which terrorist groups move money internationally can still be enhanced. Collaborative working within regions or focusing on specific terrorist risks is increasing knowledge in this regard. This is another reason why countries should focus greater energy on strengthening cross-border partnerships with CTF counterparts.

Adapting CTF policies to developing threats, including the 'internationalisation' of extreme right-wing terror

The global CTF regime was designed to combat jihadist terrorism following the 9/11 attacks. Yet the profile of the terrorist threat faced today is multifaceted; the CTF strategy developed by LEAs and security services must therefore adapt. For example, understanding the funding methods of jihadi-inspired lone actors and small cells or those of the extreme right wing must be improved as a priority. Terrorist risks that have been traditionally viewed as 'domestic' must be carefully monitored for the emergence of cross-border activity; international CTF partnerships need to be developed to ensure transnational connections can be identified and addressed where necessary.

186. The Counter ISIL Finance Group was formed in 2015 'to agree on an Action Plan to further their understanding of ISIL's financial and economic activities, share relevant information, and develop and coordinate efforts to combat ISIL's financial activities'. See US Department of State, 'Establishment of the Counter-ISIL Finance Group in Rome, Italy', press release, 20 March 2015, <https://2009-2017.state.gov/r/pa/prs/ps/2015/03/239592.htm>, accessed 23 August 2019.
187. Tom Keatinge, 'Reinvigorating the Forgotten Financial Fight Against Al-Shabaab', *RUSI Commentary*, 8 May 2019.

III. New Technologies and Terrorism Finance

THUS FAR, THIS paper has considered the conceptual objectives of the CTF regime and illustrated the importance of developing risk-based CTF responses. Consistent with the objective of this paper to consider the response to terrorist financing through a risk-based lens, a further element that deserves consideration is the role of new technologies – technologies that did not exist when the post-9/11 CTF regime was designed.

As the UN's Counterterrorism Executive Directorate has noted, as financial and communication technologies have proliferated in the 21st century, member states should 'review the relevance and effectiveness of existing tools to counter the financing of terrorism'.[188] It is therefore pertinent to consider how technology has impacted the terrorist-financing landscape. Terrorists, like criminals are often early adopters of new technology, innovating as a result of traditional methods being squeezed.[189] This chapter will assess the extent to which terrorists are relying on new financial technologies to raise, store, move and spend funds, and how the current policy and law enforcement response measures up, framed by one of the overarching questions of this paper of whether terrorist-financing responses reflect the risks faced today.

FinTech

The term FinTech is frequently used in a broad sense in public discussions, describing the increasing influence of technology in shaping financial services, and its rapid adoption by the financial sector.[190] FinTech may refer to a range of financial offerings, including peer-to-peer lending, digital wallets, money-transfer services and cryptocurrency exchanges.

Commonly viewed as 'market disruptors' and 'challengers' to legacy financial institutions, the FinTech sector is altering the landscape of finance and financial crime, which is reflected in FATF's increasing focus in recent years. Under the Argentine presidency in 2017, FATF created its FinTech and RegTech[191] Initiative, noting that FATF 'strongly supports responsible financial innovation that is in line with the AML/CFT requirements found in FATF Standards, and will

188. UN Security Council, Counterterrorism Executive Directorate (CTED), 'Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States', S/2016/49, October 2016.
189. Tom Keatinge and Kerstin Danner, 'Assessing Innovation in Terrorist Financing', *Studies in Conflict & Terrorism*, 14 January 2019, <https://doi.org/10.1080/1057610X.2018.1559516>.
190. Florence Keen and David Carlisle, 'Money Laundering and the FinTech Sector, Risks and Realities', FinTech Fincrime Exchange, 2017.
191. Regulatory Technology.

continue to explore the opportunities that new financial and regulatory technologies may present for improving the effective implementation of AML/CFT measures'.[192]

There is an important balance to be found between financial innovation and the benefits that this may deliver, such as financial inclusion, while simultaneously ensuring that new products include appropriate compliance and financial crime checks. The concern of some supervisors and FIUs is that FinTech start-ups may be more vulnerable to exploitation by illicit actors,[193] for example de-emphasising customer due diligence checks in order to increase their rate of account growth.[194] The use of pre-paid cards during the 2015 attacks in Paris[195] furthered the perception that alternative payment methods, including emerging FinTech payment solutions, are high risk. In February 2016, the European Commission declared its intention to bring forward changes to EU legislation in a further iteration of the Anti-Money Laundering Directive to address the terrorist-financing risks inherent in new technologies.[196]

Virtual currencies (also now referred to by FATF as 'virtual assets') in particular have garnered attention as a potential money-laundering and terrorist-financing risk, most recently under the US presidency of FATF in 2018–19. In its Public Statement on Mitigating the Risks from Virtual Assets, FATF recognised the need to adequately address the money-laundering and terrorist-financing risks associated with virtual asset activities and set out more detailed implementation requirements for regulation and monitoring of virtual asset service providers such as exchanges. Through a new Interpretive Note to Recommendation 15, it has clarified how FATF Standards will apply to activities or operations involving virtual assets, advising countries to consider virtual assets as 'property', 'proceeds', 'funds' or 'corresponding value'.[197]

192. FATF, 'FinTech and RegTech Initiative', <https://www.fatf-gafi.org/fintech-regtech/?hf=10&b=0&s=desc(fatf_releasedate)>, accessed 31 December 2019.
193. The Canadian FIU FINTRAC warned that FinTech companies are at greater risk of money laundering and terrorist financing, noting the most susceptible sectors as electronic payments, virtual currencies and online gambling. See Ephraim Vecina, 'Fintechs Face an Especially Grave Risk of Money Laundering – FINTRAC', *Mortgage Broker News,* 23 July 2019.
194. See, for example, *BBC News*, 'Revolut Whistleblower Had Concerns Over CEO Conduct and Compliance', 2 April 2019; Nik Storonsky, 'Let Me Set the Record Straight', Revolut CEO's blog, 1 March 2019, <https://blog.revolut.com/let-me-sec-the-record-straight/>, accessed 23 August 2019.
195. Foo Yun Chee, 'EU Proposes Stricter Rules on Bitcoin, Prepaid Cards in Terrorism Fight', *Reuters*, 5 July 2016; *Guardian,* 'Militants Using Gift Cards to Bankroll Terrorism, Intelligence Agency Says', 2 May 2017.
196. European Commission, 'Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight Against Terrorist Financing', COM (2016) 50 final, Strasbourg, 2 February 2016.
197. FATF, 'Public Statement – Mitigating Risks from Virtual Assets', 22 February 2019, <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html>, accessed 7 October 2019.

At the final FATF plenary of the US presidency held in Orlando, Florida, in June 2019, US Treasury Secretary Steven Mnuchin emphasised that virtual asset service providers must:

- 'Identify who they are sending funds on behalf of, and who is the recipient of those funds;
- Develop processes where they are required to share that information with other providers of virtual assets, and law enforcement;
- Know their customers and conduct proper due diligence to ensure they are not engaging in illicit activity; and,
- Develop risk-based programs that account for the risks in their particular type of business'.[198]

The terrorist-financing risk associated with virtual currencies was assessed in a 2018 report commissioned by the European Parliament.[199] The report, written by RUSI, found that while there was a small number of cases that reveal terrorist use of virtual currencies, likely due to their perceived anonymity and decentralised nature, adoption did *not* appear to be widespread. The primary reason for low uptake is probably linked to ease of use. Virtual currencies remain complex to operate, charge high fees and opportunities for use are limited, particularly when compared to cash. Furthermore, virtual currencies are not as anonymous as often thought, and avoiding chokepoints – such as exchanges where virtual currencies are exchanged for fiat currency (and vice versa) – that present operational vulnerabilities for terrorist users adds further risk. This is not to say that the terrorist-financing risk posed by virtual currencies is non-existent. For example, virtual currencies can facilitate the interaction between terrorist actors and OCGs via the purchase of illicit items such as weapons or fraudulent documents from the Dark Web,[200] as well as acting as a currency for online crowdfunding.[201]

If operational efficiency increases and the adoption of virtual currencies for payments and transfers becomes more widespread, this may lead to greater use by terrorist actors. Thus, although the risk posed by virtual currencies for terrorist use may currently be over-hyped,[202] it is essential that governments ensure that legal and regulatory mechanisms keep pace with advances in technology, and that financial investigators, prosecutors and judges are trained to understand how this technology works.

198. US Department of the Treasury, 'Remarks of Secretary Steven T Mnuchin, FATF Plenary Session, Orlando, Florida', 21 June 2019.
199. European Parliament, Study for the TERR Committee, 'Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating the Response', PE 604.970, May 2018.
200. Nikita Malik, *Terror in the Dark: How Terrorists use Encryption, the Darknet and Cryptocurrencies* (London: Henry Jackson Society, 2018), pp. 24–36.
201. Nathaniel Popper, 'Terrorists Turn to Bitcoin for Funding, and They're Learning Fast', *New York Times*, 18 August 2019.
202. Authors' interview with US law enforcement agency, Washington, DC, May 2019; authors' interview with Southeast Asian FIU, Jakarta, April 2019; authors' interview with European law enforcement agency, Brussels, March 2018.

Social Media

Social media is another area of technological advancement that has drawn scrutiny as a potential facilitator of terrorist financing. It was identified by FATF in 2015 as an emerging risk citing the use of networks in 'coordinating fundraising campaigns' with schemes that involve 'up to several thousand "sponsors" and may raise significant amounts of cash'.[203] In this paper social media refers to networking sites (such as Facebook), content-hosting services (such as YouTube), crowdfunding services (such as GoFundMe) and encrypted communications services (such as Telegram and WhatsApp).

A joint report in 2019 by the Asia/Pacific Group on Money Laundering and the Middle East and North Africa Financial Action Task Force (MENAFATF) (both FATF-style regional bodies) used 27 case studies to outline specific types of social media that may be vulnerable to terrorist financing:[204]

- **Social networking and content-hosting services**: to solicit donations, promote terrorism through propaganda and radicalisation.
- **Internet communication services**: to privately communicate with campaigners or terrorist groups. The vulnerabilities of these services, in particular encrypted communication and the number of active users, are factors driving their abuse for terrorist financing.
- **Crowdfunding services**: to disguise the use of funds for humanitarian causes, with services that integrate traditional and new payment services, hindering detection and investigation by competent authorities.[205]

During the course of 2019, RUSI was the lead research organisation for the Global Research Network on Terrorism and Technology.[206] As part of that project, the authors conducted a study considering the terrorist-financing vulnerabilities posed by social media.[207] This analysis argued that there has been limited focus on the potential role of social media in terrorist financing. This is despite overt calls via social media to fund terrorist fighters during the Syria conflict,[208] the

203. FATF, 'Emerging Terrorist Financing Risks'.
204. Asia/Pacific Group on Money Laundering (APG) and Middle East and North Africa Financial Action Task Force (MENAFATF), 'Social Media and Terrorism Financing', January 2019.
205. *Ibid*., p. 1.
206. For further details see Aaditya Dave and James Sullivan, 'The Global Research Network on Terrorism and Technology', <https://rusi.org/projects/global-research-network-terrorism-and-technology>, accessed 14 December 2019.
207. Tom Keatinge and Florence Keen, 'Social Media and Terrorist Financing: What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?', RUSI Global Research Network on Terrorism and Technology, Paper No. 10, undated.
208. Joby Warrick, 'Private Donations Give Edge to Islamists in Syria, Officials Say', *Washington Post,* 21 September 2013; *Kharon Brief*, 'Hayat Tahrir al-Sham Returns to Fundraising Through Social Media to Prepare "Mujahideen" for Battle', 21 August 2019.

continued operations of sanctioned individuals on platforms such as Twitter,[209] and the use of crowdfunding sites for charitable purposes.[210] The terrorist-financing vulnerabilities posed by social media have been highlighted by a number of jurisdictions, including the US in its 2018 National Risk Assessment[211] and by Indonesia, which reportedly noted in an unpublished White Paper in 2017 a changing trend in fundraising methods for terrorists, terrorist activities and organisations, from the use of NPOs in 2013–15 to the use of social media.[212]

Thus, while there is no figure for the scale of terrorist-financing activity on social-media platforms, there is clear potential for abuse,[213] and the risk is attracting high-level attention. During the Paris 'No Money for Terror' Conference in 2018, President Emmanuel Macron and the resulting conference final statement called for more active cooperation.[214] In particular, it called for cooperation between government authorities (including FIUs, LEAs, intelligence and investigation services) and the tech industry (including major internet and social-media platforms) to counter terrorism financing, recognising the changing nature of how terrorists may raise funds online and the need for public–private collaboration.

The rapid pace of development and adoption of new payment methods require policymakers to build new, and leverage existing, PPPs to ensure CTF efforts by social-media company are informed and effective.

209. Mark Nakhla, 'Terrorist Financing and Social Media', Camstoll Group, December 2016, <https://www.un.org/sc/ctc/wp-content/uploads/2016/12/TCG_Social-Media-TF_11DEC161.pdf>, accessed 31 May 2019.
210. APG/MENAFATF, 'Social Media and Terrorism Financing', p. 6.
211. US Department of the Treasury, 'US CTF National Risk Assessment', 2018, p. 2.
212. Authors' interview with law enforcement officer, Jakarta, April 2019. A 2017 White Paper produced by Indonesia's anti-money-laundering agency (PPATK) and its national counterterrorism agency (BNPT), although not publicly available, was widely reported on in the regional press, see, for example, Wahyudi Soeriaatmadja, 'Donations Via Social Media Now Main Source of Terrorism Funding in Indonesia', *Straits Times*, 18 October 2017.
213. Keatinge and Keen, 'Social Media and Terrorist Financing'.
214. Emmanuel Macron, 'No Money for Terror', speech by Emmanual Macron, President of the Republic at the International Conference on Combating the Financing of Daesh and Al-Qaeda, Paris, 26 April 2018; République Française Ministry for Europe and Foreign Affairs, 'Final Statement', International Conference on Combating the Financing of Daesh and Al-Qaeda, Paris, 26 April 2018, <https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/news-about-defence-and-security/article/final-statement-international-conference-on-combating-the-financing-of-daesh>, accessed 7 October 2019.

Recommendations

Engage more actively with risks posed by new technologies

This chapter has illuminated the potentially new ways in which terrorists may exploit the opportunities presented by new payments platforms, virtual currencies and social media to raise, move and use funds. While the scale of terrorist financing across these platforms is unquantifiable, it is important that governments, their regulators and LEAs remain attuned to innovations in terrorist financing, ensuring that standards of compliance are harmonised to prevent terrorists finding gaps in the system.

Dedicate resources to training financial investigators, prosecutors and judges in understanding the abuse of financial technologies

While the use of new payment methods and technologies by terrorists to raise funds may presently be low, their role in supporting attacks such as those in Paris in November 2015 are clear.[215] It is thus important that the law enforcement and criminal justice response is sufficiently attuned and capable when investigating and prosecuting the use of new technologies and payment methods for terrorist financing. Depending on the level of risk, jurisdictions should invest in training and capacity to develop a baseline level of understanding of FinTech, virtual currencies and social media among financial investigators, prosecutors and judges.

Develop more active CTF engagement with new payment platforms and include financial technology companies in public–private information-sharing partnerships

In addition to major financial institutions, technology companies should be included in information-sharing partnerships to ensure that the awareness of and response to terrorist financing covers all relevant stakeholders, not just members of the formal banking sector. This should include the new payments facilitators and platforms discussed in this chapter that may be abused for terrorist crowdfunding campaigns.

Drive greater focus on terrorist financing by social media companies, ensure terms of service and community standards explicitly reference and prohibit terrorist financing, and that social- media companies make interventions accordingly

Social media companies identified as higher risk for terrorist financing should engage proactively with the global CTF regime, for example by updating their terms of service and community standards to explicitly reference and outlaw terrorist financing (consistent with universally applicable international law) and actions that contravene UNSCRS and sanctions. This includes

215. Foo Yun Chee, 'EU Proposes Stricter Rules on Bitcoin, Prepaid Cards in Terrorism Fight'; *Guardian*, 'Militants Using Give Cards to Bankroll Terrorism, Intelligence Agency Says'.

ensuring social media companies understand and apply sanctions designations.[216] To underpin this strengthening of standards and governance, FATF should build on the work undertaken by two of its regional bodies[217] and prioritise raising awareness amongst its member states of the terrorist-financing vulnerabilities posed by social media, including producing specific guidance.

216. See Chris Meserole and Daniel Byman, 'Terrorist Definitions and Designations Lists: What Technology Companies Need to Know', RUSI Global Research Network on Terrorism and Technology, Paper No. 7, undated.
217. APG/MENAFATF, 'Social Media and Terrorism Financing'.

IV. Sharpening the Response

THROUGHOUT THIS PROJECT, the authors have sought to identify evidence of, or principles contributing to, CTF effectiveness, a notion that is highly challenging to measure. Some interviewees proposed best practices that should be promoted and adapted for use around the world; others confirmed the view expressed by one European FIU director that many countries, including his own, are 'sleepwalking' when it comes to combating terrorist financing.[218] In his view, these countries are doing about enough to meet FATF's requirements, but not considering the realities of the challenges faced in their own country.

This issue is underlined by Annex A of FATF's 'Terrorist Financing Risk Assessment Guidance', which details the extent to which countries have published a standalone terrorist-financing risk assessment – only nine of the 56 countries featured in the analysis.[219] Many terrorist-financing risk assessments are subsumed into wider anti-money-laundering risk assessments, often treating terrorist financing as an adjunct to money laundering, rather than a specific risk category that needs to be individually assessed. This failure to apply a dedicated focus to terrorist financing means that it is only when a terrorist attack occurs, and financial evidence reveals links and activities that could have been critical to preventing the attack, that the difference between CTF theory and practice becomes clear.[220]

FATF's Shift Towards Effectiveness

The only public process that attempts to assess the effectiveness of countries' responses to terrorist financing is FATF's mutual evaluation programme.[221] Conducted every seven to 10 years, this process has assessed not only 'technical compliance' (does a country have the laws and agencies in place for tackling money laundering and terrorist financing?), but since 2012 has also attempted to assess effectiveness.

In its most recent methodology, FATF defines effectiveness as the extent to which the legal and institutional framework is producing the expected results and that FATF-defined outcomes are achieved. The assessment is intended to '(a) improve FATF's focus on outcomes; (b) identify the extent to which the national AML/CTF system is achieving the objectives of FATF standards

218. Authors' interview with EU member state FIU director, London, February 2018.
219. FATF, 'Terrorist Financing Risk Assessment Guidance', July 2019, pp. 54–56.
220. Authors' interview with law enforcement official, Brussels, February 2018.
221. It should be noted that UNSCR 1373 requires the Counterterrorism Committee (CTC) to monitor the implementation of its provisions. Expert assessments are undertaken by the CTC's Executive Directorate (CTED). These 'Detailed Implementation Assessments' are shared only with the country under review.

and identify systemic weaknesses; and (c) enable countries to prioritise measures to improve their system'.[222]

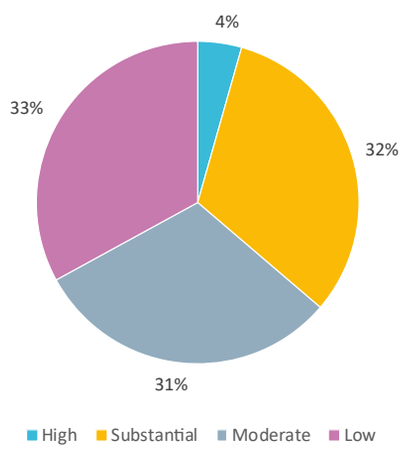
The relevance and effectiveness of FATF's assessments has been widely reviewed and is not within the scope of this paper.[223] However, for terrorist financing, the most relevant measures of CTF effectiveness are FATF's Immediate Outcomes (IOs) 9 and 10. IO9 states that 'terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions. ... When appropriate, terrorist financing is pursued as a distinct criminal activity and financial investigations are conducted to support counter terrorism investigations'.[224] IO10 seeks to determine the extent to which countries ensure that '[t]errorists, terrorist organisations and terrorist support networks are identified and deprived of the resources and means to finance or support terrorist activities and organisations'.[225] Connected with this, FATF also considers whether a country has a good understanding of its terrorist-financing risks and 'takes appropriate and proportionate actions to mitigate those risks, including measures that prevent the raising and moving of funds through entities or methods which are at greatest risk of being misused by terrorists', including charities.[226]

So how exactly have countries been scoring on CTF effectiveness thus far? Of the 91 FATF and FATF-style regional body countries (as of 7 January 2020) that have undergone their fourth-round Mutual Evaluation Reports (MER), only 4% and 2% have achieved a high level of effectiveness (see Figures 2 and 3) under IO9 and IO10, respectively. While substantial, moderate and low effectiveness were relatively evenly split for IO9, meaning that nearly two-thirds of the countries assessed to date require significant improvements to be considered highly effective, over 80% of countries require significant improvements under IO10 to reach the required standard.[227]

---

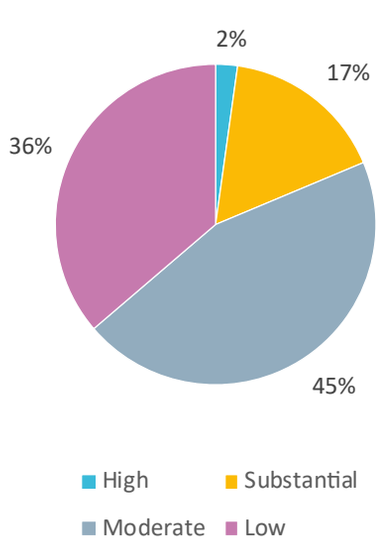
222. FATF, 'Methodology for Assessing Technical Compliance with FATF Recommendations and the Effectiveness of AML/CFT Systems', updated October 2019, pp. 15–16.
223. Ronald Pol, 'Anti-Money Laundering Effectiveness: Assessing Outcomes or Ticking Boxes?', *Journal of Money Laundering Control* (Vol. 21, No. 2, 2018), pp. 215–30; Matthew Redhead, 'Deep Impact? Refocusing the Anti-Money Laundering Model on Evidence and Outcomes', *RUSI Occasional Papers* (October 2018); Mara Wesseling and Marieke de Geode, 'Counter Terrorism Financing Policies in The Netherlands: Effectiveness and Effects (2013-2016)', Amsterdam Institute for Social Science Research, December 2018, <https://www.wodc.nl/binaries/2689D_Summary_tcm28-372746.pdf>, accessed 1 January 2020.
224. FATF, 'Methodology for Assessing Technical Compliance with FATF Recommendations and the Effectiveness of AML/CFT Systems', p. 124.
225. *Ibid*., p. 126.
226. *Ibid*.
227. Pie-chart data is based on the initial Mutual Evaluation Report of each of the 91 countries assessed thus far as per data provided by FATF. See FATF, 'Consolidated Assessment Ratings', <https://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html>, accessed 14 January 2020.

Figure 2: Immediate Outcome 9



Source: FATF, 'Consolidated Assessment Ratings', <https://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html>, accessed 14 January 2020.

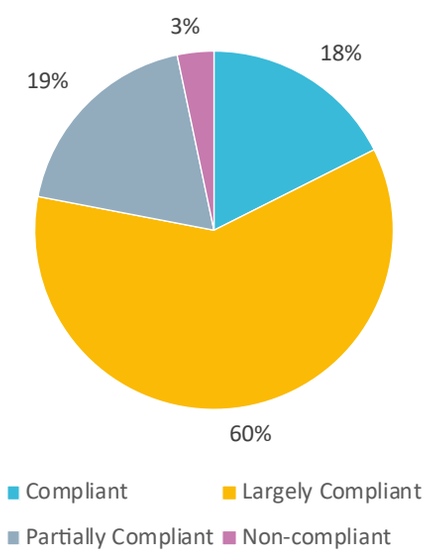
Figure 3: Immediate Outcome 10



Source: FATF, 'Consolidated Assessment Ratings'.

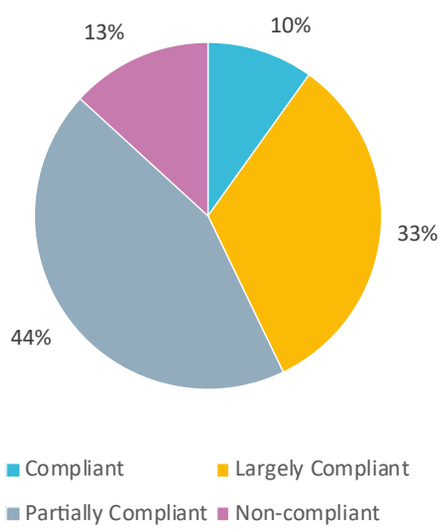
While the CTF-relevant elements of technical compliance, including the criminalisation of terrorism finance (Recommendation 5) and the implementation of targeted financial sanctions (Recommendation 6), reveal a more positive picture (see Figures 4 and 5), with only a small number of countries (3% and 13%, respectively) achieving 'non-compliance', it is clear from the IO data that effective implementation via the appropriate deployment of these CTF tools is considerably more challenging than mere technical compliance. Furthermore, in both cases, despite the low level of non-compliance, only 18% and 10% of countries, respectively, are fully compliant.

Figure 4: Recommendation 5



Source: FATF, 'Consolidated Assessment Ratings'.

Figure 5: Recommendation 6



Source: FATF, 'Consolidated Assessment Ratings'.

Box 4: The UK's Mutual Evaluation Report 2018: Counter Terrorist Financing

One of the few countries to achieve a highly effective rating for IO9 in its fourth-round Mutual Evaluation Report (MER) is the UK, reflecting the highly positive review of the UK's CTF architecture. While the design of a CTF regime should reflect the risks faced by an individual country, the UK provides a valuable case study from which to draw lessons. In summary, the UK MER notes:

- The UK proactively and systematically investigates terrorism finance alongside terrorism-related investigations, with cases that show a range of terrorist-financing activity is pursued, and that terrorism finance is a distinct criminal activity.
- Terrorist-financing investigations are well integrated into broader counterterrorism strategies, with good coordination between agencies, across jurisdictions, regions and sectors.
- CTF authorities have a close and fruitful relationship with financial institutions and NPOs.
- The UK has demonstrated its ability and willingness to use all available measures to disrupt terrorism finance, evidenced by LEAs in Northern Ireland adapting to the changing and specific nature of terrorism finance by pursuing alternative offences, for example, in relation to organised crime (see example below from the MER).

- JMLIT is a particularly positive feature of the UK system, demonstrating strong public–private partnership on terrorist-finance investigations.[i]

Disrupting Terrorist Financing in Northern Ireland

Since the signing of the Belfast Agreement in 1998, the nature of terrorist financing in Northern Ireland has evolved with paramilitary and terrorist groups increasingly focusing on organised crime, not all of which is intended to raise funds for terrorism. Dissident Republican groups in Northern Ireland undertake a range of criminal activities, including cigarette smuggling, fuel laundering and smuggling, extortion and robbery. These groups operate as OCGs. While some of their conduct may be committed for the purpose of funding terrorist activity, some may also be committed for personal gain.

By focusing on organised crime, Northern Ireland's authorities are therefore able to prosecute and disrupt potential terrorist groups engaged in potential terrorist-financing activity. LEAs operating in Northern Ireland collaborate in an Organised Crime Task Force, which targets organised crime in the province. Dissident groups often move the proceeds of their organised criminal offending across the border either to or from their counterparts in the Republic of Ireland. Acknowledging the terrorist-financing (and money-laundering) risk posed by cross-border cash transfers and MSBs in Northern Ireland, the Task Force established a programme to visit money-service banks located close to the Irish border to understand their particular compliance challenges. The police service of Northern Ireland, the National Crime Agency and HMRC also established a co-located Paramilitary Crime Taskforce in 2017. The programme has already resulted in the financial scoping of more than 40 cases of individuals linked to paramilitary crime.

i. FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom', Mutual Evaluation Report, December 2018, p. 85.

The impact of FATF's shift towards evaluating effectiveness alongside technical compliance has encouraged an extensive debate.[228] As relates to CTF, some interviewees felt that there was a need to move beyond focusing merely on FATF-defined effectiveness. One CTF law enforcement officer argued that to be truly effective means ensuring jurisdictions understand and demonstrate what the threat means to them, beyond the emphasis FATF has placed on the jihadi terrorist risk in recent years.[229] A policy adviser noted that the Mutual Evaluation process can prevent countries from prioritising their terrorist-financing risk, focusing instead on box-ticking to gain a good score.[230] Additional concerns included a belief that the FATF model

228. A range of academics have addressed this issue, including Pol, 'Anti-Money Laundering Effectiveness', and Tom Keatinge, 'The Financial Action Task Force Should Embrace the Opportunity to Reform', *RUSI Commentary*, 25 June 2019.
229. Authors' interview with Canadian law enforcement officer, Ottawa, October 2017.
230. Authors' interview with Canadian policy adviser, Ottawa, October 2017.

ends up *dictating* risk, as opposed to *encouraging* the risk-based approach[231] and developing a rounded understanding of terrorist-financing risks.[232]

It is important to note that within FATF Methodology, Recommendation 1 requires that countries:

> ...should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.[233]

As a result, most countries have produced national risk assessments (not all of which are made public) as part of this risk assessment, yet few states address terrorist financing as a standalone risk, choosing instead to conflate its consideration with the wider assessment of money laundering.[234] The effectiveness of the risk-based approach is then assessed via FATF IO1 to determine whether '[M]oney laundering and terrorist financing risks are understood'.[235] Assessors are expected to consider the process by which the risk assessment was conducted and the reasonableness of its findings, but are not expected to conduct their own risk assessment.[236]

Many interviewees operating within the CTF regime, be they financial investigators or law enforcement officials, queried the effectiveness of FATF's methodology for assessing CTF regimes. There are several possible reasons for this. First, there is inevitably a degree of interviewee bias in their perception of FATF, which may be influenced by the jurisdiction in which they operate or their experience of FATF and any rating they have received. It may also indicate a lack of awareness of FATF methodology, particularly given the extent to which countries have failed to disaggregate their responses to money laundering and terrorist financing.

But these concerns may also indicate a more fundamental issue. Researchers at the University of Amsterdam have argued that it is unclear what FATF considers to be evidence, questioning if indicators such as the number of prosecutions are appropriate measures of effectiveness, and whether preventive and innovative initiatives are sufficiently appreciated within the evaluation.[237] A leading terrorist-financing prosecutor argues that measuring the number of arrests, prosecutions and convictions is a poor assessment of success, and that if these indicators

231. Authors' interview with a Ministry of Finance official from an EU member state, The Netherlands, November 2017.
232. Authors' interview with financial crime policymaker, Kathmandu, July 2018.
233. FATF, 'The International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', p. 9.
234. FATF, 'Terrorist Financing Risk Assessment Guidance', pp. 54–56.
235. FATF, 'Methodology for Assessing Technical Compliance with FATF Recommendations and the Effectiveness of AML/CFT Systems', p. 93.
236. *Ibid*., p. 8.
237. Wesseling and de Goede, 'Counter Terrorism Financing Policies in The Netherlands'.

are accepted, there is no jurisdiction in the world that could claim to be truly effective.[238] The same interviewee proposed being more creative with measurement indicators, such as considering the amount of financial information shared pre- and post-attack (public–public and public–private), particularly if that information leads to exposing and disrupting a network.

While FATF is the central standard-setting body,[239] it relies on the work of its FSRBs for input, provision of technical assistance and assessments of its members.[240] Throughout this project, the authors have had the opportunity to interact with a number of the FSRBs, and found best practices – such as hosting typology meetings – through which regions have taken steps to proactively identify terrorist-financing risks, and collectively formulate a response. Furthermore, during the life of this project, several FSRBs have published CTF operational plans, revealing the extent to which responses to terrorist financing remain far from being effective.[241]

A recent, positive trend can be observed in Southeast Asia where a group of countries have sought to move beyond the baseline CTF requirements of FATF (see Box 4).

Box 4: Southeast Asia CTF Summit and Regional Risk Assessments

The Australian FIU, AUSTRAC, and the Indonesian FIU co-lead the annual Southeast Asian Counter Terrorist Financing Summit, which began in Sydney in 2015 to promote regional cooperation and collaboration between FIUs in the Southeast Asia region.

On the basis of this group, the region published its Regional Risk Assessment on Terrorism Finance in 2016, which identified four priority areas:

- Self-funding from legitimate sources.
- At-risk NPOs.
- Cross-border movement of funds/value.
- External funding into the region.[i]

Over the following 12 months, the group produced its 'Non-Profit Organisations & Terrorism Financing: South East Asia Regional Risk Assessment 2017',[ii] noting that the regional risk of terrorist financing

238. Authors' interview with senior terrorist-financing prosecutor, Brussels, November 2017.
239. FATF's primacy has recently been challenged by the European Commission, which published its own high-risk country list in February 2019. The list proved highly controversial, receiving sharp criticism from the US Treasury and was opposed by most EU member states on the basis of its methodology. The list was withdrawn, but it is likely to return once the methodology has been revised.
240. FATF, 'High-Level Principles and Objectives for FATF and FATF-Style Regional Bodies', updated February 2019.
241. See, for example, Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), 'Regional Counterterrorist Financing Operational Plan (2018/2020)', Plen.doc 6, 2018.

through NPOs is 'medium' overall. However, in the case of Indonesia, NPOs have been linked in many investigations to larger terrorist groups, and appear to have been a 'significant vehicle'[iii] for terrorist financing in support of individuals and networks. High-risk subsets included NPOs with a high volume of cash; public donations as the main source of funds (including membership fees); those operating in or sending funds to high-risk jurisdictions; and those that support a particular ethnicity or religion.

The report outlines priority actions based on the main areas of risk, vulnerability and overall terrorist-financing risk, including:

- Cross-border information sharing based on regional risks.
- Development of red-flag indicators of high-risk NPO activity.
- Greater vetting of NPO staff and directors.
- Identification of unregulated NPOs.
- Risk-based supervision of NPOs to provide greater oversight and disruption of NPOs at risk of terrorist financing.

This form of granular assessment, with risks, vulnerabilities and priority actions laid out for CTF stakeholders, reveals the art of the possible when jurisdictions work together on shared priorities. While the region is not unique in this regard, regional summits and risk assessments such as this are not yet commonplace.

The community continues to grow, with more than 350 representatives from 29 countries attending the 2018 Counterterrorism Financing Summit in Manila.[iv] The summit has also spawned a range of working groups that operate throughout the year to help develop understanding of and capacity to tackle the terrorist-financing risks that confront the region.[v]

i. Australian Government, 'South East Asia & Australia Regional Risk Assessment 2016', <https://www.austrac.gov.au/sites/default/files/2019-07/regional-risk-assessment-SMALL_0.pdf>, accessed 1 January 2020.
ii. Commonwealth of Australia, 'Non-Profit Organisations & Terrorism Financing: South East Asia Regional Risk Assessment 2017', <https://www.austrac.gov.au/sites/default/files/2019-06/regional-NPO-risk-assessment-WEB-READY_ss.pdf>, accessed 1 January 2020.
iii. *Ibid*., p. 4.
iv. Australian Government, 'The Manila Communiqué', Counterterrorism Financing Summit, Manila, November 2019, <https://www.austrac.gov.au/about-us/our-recent-work/5th-regional-counter-terrorism-financing-summit-manila-communique>, accessed 1 February 2020.
v. *Ibid*.

Taking Ownership

One UK private sector interviewee described how jurisdictions fail to take real ownership unless terrorism is on their doorstep.[242] The financial war waged against Islamic State is a case in point. Western powers, in response to many of their own citizens travelling to Iraq and Syria as foreign fighters, as well as the spike in terrorist activity in the name of Islamic State, focused the West's CTF priorities in a manner that had not been seen since 9/11. CTF 'mattered' as it was perceived as both a direct threat to Western society, as well as an imminent threat to their citizens' lives. The creation of a global coalition to combat ISIL financing, the CIFG, should act as a model against other, transnational threats such as Boko Haram or Al-Shabaab.

The gap between those who perceive and thus respond to terrorist-financing threats and those who do not is evident. According to one former FIU head,[243] jurisdictions without a local threat of terrorist attacks often do not consider 'financial outflows' or their role facilitating the global movement of terrorist financing[244] as part of their terrorist-financing risk assessment, because once the funds leave or pass through their jurisdiction they are no longer perceived to be their problem. This example is central to the question of CTF effectiveness. Is the global response sufficiently nuanced to ensure that each country is contributing to the global effort to combat global threats in a coordinated fashion? Or are responses generic, lacking structure and direction that reflect the contribution the country can make to this global effort?

As has been demonstrated throughout this paper, terrorist financing is multi-layered. Terrorist actors employ a range of different financing strategies depending on their status, organisational structure and the fundraising resources, such as commodities they control, businesses they run or diaspora support at their disposal. In turn, this multi-faceted picture requires a multi-dimensional response from LEAs and policymakers. Judging the success of CTF measures by reference to the wrong objective will produce an ineffective outcome. Indeed, the regime has been wrongly criticised by some on the basis that financial tools cannot stop actors from driving cars into pedestrians, or a group such as Islamic State from amassing income through its own territory.[245] Policymakers and academics should continually scrutinise the current system through the prism of effectiveness, and be open-minded to innovative measures of success in addition to traditional indicators.

---

242. Authors' interview with UK head of financial crime compliance in the private sector, London, January 2018.
243. Authors' interview with former FIU director, Middle East, February 2019.
244. A recent report from the Luxembourg FIU highlights the importance of international cooperation and financial centres engaging with the global CTF regime, noting that 90% of terrorist-financing reports made to the Luxembourg FIU had no connection with Luxembourg. See Cellule de Renseignement Financier (CRF – French FIU), '2018 Report on the Activity of the French Financial Intelligence Unit', October 2019.
245. Neumann, 'Don't Follow the Money: The Problem with the War on Terrorist Financing'.

Recommendations

Clarify the objectives of CTF measures

CTF measures can aim to: (1) minimise access to resources; (2) bring terrorist financiers to account; and (3) maximise the impact of financial intelligence in counterterrorism cases. Depending on the context, only one or two of these objectives may be applicable:

- Although not entirely redundant, objectives (2) and (3) are less applicable to territory-controlling groups because they are de facto beyond law enforcement reach.
- In contrast, (1) is largely inapplicable to lone actors given the small amounts of funds required.

It is imperative that the CTF regime is risk-based and includes not only financial measures. For instance, terrorist access to resources can be minimised through military action, making it more difficult for terrorists to purchase goods they need (such as chemicals) or to sell commodities they control (such as oil).

Governments should promote better public and expert awareness of CTF objectives so as to minimise unjustified scepticism, for instance, the argument that CTF measures are ineffective because terrorist attacks still happen.

Conduct terrorist-financing-dedicated national and regional risk assessments via regional FATF bodies and tailored risk assessments

While the top-down approach to CTF developed by FATF remains central, countries and regions should be encouraged to consider their specific terrorist-financing risks and appropriate responses through national and regional risk assessments, for example via the work of the FSRBs or sub-regional groups such as the Southeast Asian CTF Summit. CTF action must be risk-based and reflect geographic variation. For example, in 2018, the Eurasian Group and Asia-Pacific Group FSRBs came together in Novosibirsk for a typologies workshop – which the authors attended – on terrorist financing using the proceeds of crime, including organised crime,[246] demonstrating successful cross-FSRB working on shared threats.

Furthermore, financial centres should be aware of the role they may play in facilitating the global flow of terrorist financing and conduct appropriate risk assessments.

246. Eurasia Group, 'Joint EAG/APG Typologies Workshop', 23 August 2018.

Conclusion

AS NOTED EARLIER, the 9/11 Commission Report proposed that government agencies should 'expect less from trying to dry up terrorist money and more from following the money for intelligence, as a tool to hunt terrorists, understand their networks, and disrupt their activities'.[247] From the research conducted over the past two years, in the face of a terrorism threat that has evolved considerably from that presented by Al-Qa'ida, it would seem that for many charged with implementing the global CTF regime on both a national and international basis, this advice has been forgotten. While this is perhaps understandable given the attraction – albeit most often erroneous – of the idea of severing a terrorist group's financial lifeline, the result is a less effective CTF regime.

In a November 2018 speech, FATF's executive secretary, David Lewis, noted that 'as criminals and terrorists continue to evolve, the challenge of effective implementation [of responses to terrorist financing] is only going to increase', and that the international CTF community must 'seek to evolve with them, and where possible to anticipate their moves in advance and take pre-emptive action'.[248]

Echoing this sentiment, in its updated 'Mandate' document published in April 2019, FATF notes that: 'The nature and scale of terrorist financing continues to evolve rapidly' and commits to leading the global CTF effort, providing 'a flexible and dynamic response to new threats and [taking] effective action to improve understanding, mitigation, and disruption of the risks identified'.[249] This is a commitment that the authors welcome and which may start to address the somnambulant approach taken by many countries and their law enforcement agencies and relevant private sector actors. Addressing the continued conflation of AML and CTF as one six-letter acronym rather than two – often – distinct threats demanding differing responses must be a priority. Greater national ownership to tackle terrorist financing is also needed. As one interviewee noted, 'taking action against risks that are identified for you, for example by a UN sanctions regime, is much easier than identifying your own risks and taking the necessary legal and operational steps'.[250]

Alongside the work of FATF, at the international level there is evident recognition that the implementation of the global CTF regime is deficient. UNSCR 2462 (2019) prioritised financial intelligence sharing, risk assessments and PPPs as means to combat terrorist financing. The operating paragraphs of this Resolution reveal the extent to which the response to terrorist

247. The 9/11 Commission Report, 'Final Report of the National Commission on Terrorist Attacks Upon the United States', pp. 18–19.
248. FATF, 'Speech Delivered by FATF Executive Secretary David Lewis', Southeast Asia Counterterrorism Financing Summit, Bangkok, 8 November 2018.
249. FATF, 'Mandate', 12 April 2019, p. 1.
250. Authors' interview, global CTF policymaker, London, September 2019.

financing needs to move beyond an approach that remains rooted in the post-9/11 regime. In May 2019, the authors met representatives of several Permanent Missions to the UN in New York to discuss the content of the new Resolution. While some felt that it was premature as the requirements of previous CTF resolutions still remained unmet by many countries,[251] it does offer refreshed thinking on terrorist-financing threats, highlighting ways in which the CTF regime must adapt to face down these threats.

The Resolution also provides a useful platform from which to consider the progress the international community has made from four perspectives:

- **International strategic**: the effectiveness of FATF and the growing architecture of UN bodies focused on terrorist financing as well as international initiatives such as the 'No Money for Terror' Conference and the annual Southeast Asia CTF Summit.
- **International operational**: calling for greater cross-border collaboration and information sharing.
- **National strategic**: conducting risk assessments; ensuring the financial intelligence unit and other relevant agencies are properly resourced; and establishing the necessary cross-government and PPPs.
- **National operational**: ensuring parallel financial investigations are conducted after a terrorist attack; exploiting financial intelligence; targeting criminal fundraising opportunities that may be abused by terrorists; engaging with new payment providers (FinTech) and social media companies to reduce terrorist-financing vulnerabilities.

As the research conducted for this paper demonstrates, an assessment of the global CTF regime from these four perspectives reveals a mixed picture. For 20 years, the international community has championed the importance of tackling terrorist financing. Many conferences have been held – and will continue to be – and some regional operational collaboration can be identified, but much more needs to be done to ensure countries collaborate effectively on their combined CTF endeavour. More must be done to inform that collaboration and resulting response through a better understanding of the specific nature of the finances related to different terrorist threats.

The existing CTF regime was promoted and built 'from the top down' by institutions such as the UN and FATF. That was certainly the right place to start. But, to be effective and adapt to the evolving nature of the terrorist financing threat, greater emphasis must now be placed on the development of a bottom-up approach. Such an approach will create a sharper image of the nature of the threat the global CTF regime is endeavouring to identify and disrupt, resulting in a more effective response to the continuing threat posed by terrorist financing.

---

251. It is worth noting that UNSCR 2462 'invites Member States to submit to [UNCTED and the 1267 Monitoring Team] in writing, by the end of 2019, information on actions taken to disrupt terrorist financing'. Although this is not an obligation, it may provide further insight into the extent to which countries are genuinely tackling terrorist financing.

About the Authors

Tom Keatinge is the founding Director of the Centre for Financial Crime and Security Studies at RUSI.

Florence Keen is a Research Fellow at the International Centre for the Study of Radicalisation, King's College London, specialising in far-right extremism and violence.