RUSI EUROPE

Project craaft

Collaboration, Research & Analysis Against the Financing of Terrorism

Occasional Paper

Bit by Bit

Impacts of New Technologies on Terrorism Financing Risks

Stephen Reimer and Matthew Redhead

Bit by Bit

Impacts of New Technologies on Terrorism Financing Risks

Stephen Reimer and Matthew Redhead

RUSI Occasional Paper, April 2022

Based in Brussels, RUSI Europe studies, promotes, debates and reports on all issues relating to international defence and security in Europe and abroad. RUSI Europe collaborates closely with its international parent organisation, RUSI, by exchanging expertise and by developing relationships with international stakeholders.

191 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 191 years.

This project was funded by the European Union's Internal Security Fund – Police

Published in 2022 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, April 2022. ISSN 2397-0286 (Online).

RUSI Europe
Avenue des Arts 46
1000 Brussels
Belgium
+32 (0)2 315 36 34
www.rusieurope.eu

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

The authors would like to thank Tom Keatinge, Olivia Kearney, Alanna Putze and Kinga Redlowska for their support of this research project, and Gemma Rogers for facilitating a webinar discussion where initial findings of this research in relation to online crowdfunding were presented and discussed. The research for this publication forms part of Project CRAAFT (Collaboration, Research and Analysis Against the Financing of Terrorism).

About Project CRAAFT

Project CRAAFT is an academic research and community-building initiative designed to build stronger, more coordinated counterterrorist-financing capacity across the EU and in its neighbourhood. Project CRAAFT is funded by the EU's Internal Security Fund – Police, and implemented by a Consortium led by RUSI Europe, along with the University of Amsterdam, Bratislava-based think tank GLOBSEC and the International Centre for Counter-Terrorism (ICCT), based in The Hague. For more information, visit <projectcraaft.eu>.

Executive Summary

THE POTENTIAL ROLE that new technologies – from financial technology to social media – can play in terrorist financing (TF) has been a growing subject of anxiety in European policymaking circles. With their focus on speed, efficiency and a positive user experience, new technologies not only have the potential to make life easier for ordinary consumers, but also to reduce the frictions terrorist financiers face when funding attacks and organisational activities. Virtual assets (VAs) – especially cryptocurrencies – have been a major area of concern as a new frontier of TF risks.

However, the recent focus on new technologies as an avenue for TF has not led to a consensus about how great the risks are. The debate around the issue has polarised into two broad positions – one which fears the worst, suspecting that innovation will make life easier for terrorist financiers, and another, which sees new technologies as no more or less risky than pre-existing technologies or conventional financial activities. The differences of opinion are deep, and the dialogue between the two positions difficult to resolve, because of the assumptions on which they are based. In the first case, policymakers and the traditional financial services sector tend to see novelty and uncertainty, and assess that the safest approach is to assume theoretical vulnerabilities and inherent risks are real until otherwise proved. In the second, those involved in creating and deploying new technology tend to believe that the risks should not be assumed, and need to be demonstrated. For both sides, understanding the nature and quality of evidence is essential.

Amid this debate, this paper investigates whether new technologies pose new, or exacerbate existing, TF risks in Europe. Although there were difficulties in collecting data on sensitive terrorist cases, a clearer picture still emerged: new financial technologies have indeed been used in the procurement and financing of attacks, but only with certainty in a small proportion of cases. Likewise, payment platforms, social media crowdfunding and VAs have become tools for wider organisational financing, but they have been added to, rather than replaced, well-worn and conventional methods such as cash, the use of intermediaries, or money service businesses.

Overall, new technologies have become a part of TF activities within Europe, but in a less transformational way than many policymakers feared.

Introduction

IN 1992, A British man from south London, Babar Ahmad, witnessed the horrific violence perpetrated against Bosnian Muslims while serving as an aid worker in the Balkans.[1] Later, he set up a website, primarily to publish stories about conflicts in Bosnia and Chechnya, but which also called for support, financial and otherwise, for the Taliban in Afghanistan.[2] Since then, uses of the internet for terrorism financing (TF) have evolved in step with the popularisation of new internet-enabled technologies. Online chat rooms have given way to instant messaging platforms, just like dedicated websites have been replaced by social media as a means of reaching a wide audience of sympathetic supporters.

Of particular concern today are a handful of technologies that, with their intersection with the financial system, are seen to pose distinct TF risks. The risks of virtual assets (VAs) have been widely discussed, as has the TF potential of online crowdfunding platforms.[3] Less well-defined are the risks posed by FinTech products and services, including challenger banks and the payment service providers that underpin much of the modern financial system.

Social media (like social networking sites and content-hosting platforms) and online communications tools can also be misused to support TF activities. Other innovations, such as e-commerce websites, have featured in the operational planning of self-activating terrorists in Europe, for example, in the procurement of parts for the improvised explosive device used in the Manchester Arena bombing in 2017.[4] However, the risk posed by VAs, crowdfunding, FinTech and social media cover a broader range of illicit activity, including the collection of donations and the movement and obfuscation of funds.

This paper seeks to contribute to the existing knowledge base on the degree of material threat stemming from the exploitation of new technologies, by asking to what extent new technologies have posed new, or exacerbated existing, TF risks in Europe. At present, there appears to be an obsession with the perceived vulnerabilities of new technologies, but on the basis of a

1. Robert Verkaik, 'The Trials of Babar Ahmad: From Jihad in Bosnia to a US Prison via Met Brutality', *The Observer*, 19 March 2016.
2. Michael Jacobson, 'Terrorist Financing and the Internet', *Studies in Conflict and Terrorism* (Vol. 33, No. 4, 2010), pp. 353–63.
3. Tom Keatinge, David Carlisle and Florence Keen, 'Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses', May 2018, <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf>, accessed 24 March 2021; Stephen Reimer and Matthew Redhead, 'Following the Crowd: Clarifying Terrorism Financing Risk in European Crowdfunding', Research Briefing No. 7, Project CRAAFT, 2021.
4. Stephen Reimer and Matthew Redhead, 'A New Normal: Countering the Financing of Self-Activating Terrorism in Europe', *RUSI Occasional Papers* (May 2021), p. 13.

growing – though still limited – body of evidence, the threat seems exaggerated. While new technologies have created fresh opportunities for TF, they are additional tools for an existing kitbag rather than a complete replacement set. This is particularly important given the way in which the debate on the dangers of new technologies has often developed, yielding reflexive counterterrorism financing (CTF) responses that are not neccesarily commensurate with the apparent risks.

The paper consists of four chapters. Chapter I provides a background discussion of the new technologies considered in this study and a primer on TF behaviours and objectives. Chapter II considers the TF threats posed by financial and non-financial technologies, while responses to these threats by the public and private sectors are included in Chapter III. Chapter IV evaluates the state of the threat and current responses, and the paper concludes with a series of recommendations for the European Commission on how to better track the evolving threat and improve responses at the EU and member state level.

Methodology

This project ran from January 2021 to March 2022, beginning with a targeted literature review of English-language sources, including academic articles, think tank research reports, and media articles such as news reports and opinion pieces that stake out the current policy debate in the field. Terrorist activity inspired by Islamist and far-right extremism was considered in an international context, given the transnational nature of internet-based technologies and limited literature on Europe specifically. Research gaps identified in the literature review informed the research questions and overall design of this study.

Data collection was carried out in two modes:

- Twenty-five **expert consultations** were conducted remotely due to coronavirus restrictions on international travel. Experts from the public, private and third sectors – primarily but not exclusively from western Europe – took part in semi-structured interviews regarding their experience with the scale of abuse of new technologies for TF and responses to it.
- Two **open source data-collection exercises** recorded details of a total of 261 unique events linked to terrorist events or activities in Europe between January 2015 and November 2021.
    - The first exercise focused solely on **financing for attack planning (operational financing)**, including actual, failed and planned attacks.[5] 212 attacks or plots were recorded, with 137 cases (65%) involving Islamist extremists, followed by the extreme left wing (36, or 17%), extreme right wing (36, or 17%), state-backed extremists (2, or <1%), and nationalist separatist extremists (1, or <1%).

5. Events were recorded in 19 countries: Austria, Belgium, Bulgaria, Croatia, Denmark, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Spain, Sweden, Switzerland and the UK.

- The second exercise looked at the **financing of terrorist organisations (organisational financing)**, explicitly at cases that have led to law enforcement action and potentially also to judicial proceedings against individuals.[6] Forty-nine cases were recorded, all but two of which involved Islamist extremists.

Limitations of this research design include restricted access to information held by the public sector on actual instances of terrorists or their supporters abusing new technologies for financing purposes. The authors experienced low take-up of interview requests from public sector actors, recognising that interviews hosted online may have made it difficult for public sector actors to engage fully with the research process. In addition, this might have reflected a lack of information to share; one senior head of a national financial intelligence unit (FIU) remarked that knowledge on this topic was low across European law enforcement agencies.[7] The open source data-collection exercises were hindered by the omission of financial and logistical details of financing events from reports in the public domain, usually because of legal impediments to doing so (such as privacy laws or interest in protecting ongoing investigations) or because such information is perceived to not be of interest to the public. These limitations may affect geographic biases, with some countries being over- or under-represented in the data. Timescales also caused distortions in the data on organisational financing: the period of study (2015–21) did not yield as many events concerning right-wing terrorism as expected, possibly due to the lag time between the event and when investigation may lead to judicial action.

Of course, these limitations leave open the possibility that there is a higher incidence of TF among some new technologies than the research has been able to identify. More data would inevitably provide a more nuanced view, though it seems unlikely that such material would lead to a different conclusion.

Unpacking Concepts: New Technologies

The term 'new technology' is widely used but ill defined,[8] and can in theory refer to any new tool developed in the recent past for any purpose, from instant messaging to AI. The most relevant sector to TF is known as 'FinTech', where firms use new technologies to deliver basic, data-intensive financial services quickly, securely and at a low cost. By abandoning traditional intermediaries in favour of online platforms, FinTech firms have access to a wider

6. Events were recorded in 12 countries: Bulgaria, Denmark, Estonia, France, Germany, Ireland, Italy, the Netherlands, Norway, Spain, Sweden and the UK.
7. Authors' interview with the head of an EU member state FIU, 26 July 2021.
8. For example, Recommendation 15 for the FATF Standards requires countries to 'identify and assess' money laundering and terrorism financing risks of new technologies and products. The European Commission cites this recommendation in a regulation under consideration on the traceability of crypto-assets. See European Commission, 'Regulation of the European Parliament and of the Council on Information Accompanying Transfers of Funds and Certain Crypto-Assets (Recast)', July 2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0422&from=EN>, accessed 16 March 2022.

potential market of users attracted by the convenience of undertaking financial activity online and on the go, thanks to advances in mobile technology and cellular networks.[9] FinTech firms have developed in just about every service area of the financial system, comprising:

- **Digital banking:** There are now several well-established online or 'neo' banks across Europe, such as Germany-based N26, which offer a range of the same services provided by a traditional retail bank. A growing market in business banking among digital banks has been seen in Europe as well.
- **Payments services:** Like Ireland- and US-headquartered Stripe, firms providing at least one part of the infrastructure required to process the payment of funds between individuals, businesses and/or financial institutions, either domestically or internationally.
- **Lending:** The provision of online credit, for specific purchases or more generalised personal or business loans. Some other leaders, such as the UK-based Funding Circle, use a 'peer-to-peer' (P2P) approach to funding their loans, allowing individuals to lend directly to small and medium-sized businesses, for a return.
- **Crowdfunding:** Inspired by the development of microfinancing projects in the developing world, as well as crowdsourcing of knowledge and services via the internet,[10] crowdfunding sees individuals and groups use dedicated online platforms to promote their endeavour, aggregate funds directly and send those funds to the intended recipient at speed.[11] Many such platforms – often dubbed 'returns-based' – help businesses gather capital from investors for a rate of return, or equity, in the business. In addition, donation-based platforms have developed to support charitable or other non-profit-making endeavours,[12] but these might also be thought of as a form of social media, as noted below.
- **Investments:** The investment industry has been affected by the growth of internet-based applications that allow investors to manage their portfolios directly, or with the support of automated 'robo-advisers', rather than traditional brokers.[13]

---

9. See Henri Arslanian and Fabrice Fischer, *The Future of Finance: The Impacts of FinTech, AI, and Crypto on Financial Services* (Cham: Palgrave Macmillan, 2019); Niels Pedersen, *Financial Technology: Case Studies in Fintech Innovation* (London: Kogan Page, 2021); Itay Goldstein, Wei Jiang and G Andrew Karolyi, 'To FinTech and Beyond', *Review of Financial Studies* (Vol. 32, No. 5, May 2019), pp. 1647–61; Anne-Laure Mention, 'The Future of Fintech', *Research-Technology Management* (Vol. 62, No. 4, 2019), pp. 59–63.
10. Francesca Di Pietro, 'Deciphering Crowdfunding', in Theo Lynn et al. (eds), *Disrupting Finance: FinTech and Strategy in the 21st Century* (Cham: Palgrave Macmillan, 2019), p. 2.
11. UK Crowdfunding Association, 'What is Crowdfunding?', <https://www.ukcfa.org.uk/what-is-crowdfunding/>, accessed 28 June 2021.
12. See Reimer and Redhead, 'Following the Crowd'.
13. Jake Frankenfield, 'Robo-Advisor', Investopedia, updated 21 February 2022, <https://www.investopedia.com/terms/r/roboadvisor-roboadviser.asp>, accessed 4 March 2022.

- **Insurance:** As with investments, FinTech firms have entered the insurance market with the intention of using big data and machine learning to improve risk assessments and drive down premiums.[14]
- **Virtual assets service providers (VASPs):** The VASP sector has developed out of the growth of cryptocurrencies such as Bitcoin, built on distributed ledger technology (DLT), or blockchain.[15] Such currencies have developed since Bitcoin's birth in 2008, with the growth of 'privacy coins' that have stronger encryption protocols, and 'stablecoins', anchored to an underlying asset. The core of the VASP sector currently involves the storage (in wallets) of cryptocurrencies, and their purchase and sale (through exchanges). Although there is an increasing range of goods and services that can be bought using cryptocurrencies, there are ongoing practical limitations on day-to-day use.[16] The dark net also continues to provide an alternative venue for their use, where they are the primary currency of choice.[17]

Of these FinTech 'subsectors', the most commercially prominent in Europe are digital banking, payment services and lending. According to a September 2020 survey of the top 50 European FinTech firms by valuation, payments services dominated the list with 14 entrants, followed by digital or neo banking (11) and lending (7). Investments and insurance had five and two entrants apiece, while VASPs – often seen as the most controversial subsector of FinTech – had only three.[18]

Beyond FinTech, the financial significance of social media must also be taken into account, because of its capacity to support the sharing of financial information in ways that might enable TF. According to a 2019 joint report by the Asia-Pacific Group on Money Laundering (APG) and the Middle East and North African Financial Action Task Force (MENAFATF), both FATF-style regional bodies (FSRBs) affiliated to the FATF, social media includes four sub-domains.[19]

14. Marshall Hargrave, 'Insurtech', Investopedia, updated 27 August 2020, <https://www.investopedia.com/terms/i/insurtech.asp>, accessed 4 March 2022.
15. Using a shared ledger across computer networks, Blockchain allows information about events or activities (such as financial transactions) to be stored in individual 'blocks' validated across the nodes of the network. Because of the chronological character of the chain, it is not possible to alter the data contained within retrospectively.
16. Jacob Bernstein, 'What Can You Actually Buy with Bitcoin?', *New York Times*, 3 February 2021.
17. Chainalysis, 'The 2022 Crypto Crime Report', February 2022, p. 11, <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>, accessed 4 March 2022.
18. The survey was conducted by Finovate, a FinTech events management provider. A further eight firms provided a variety of different business supports services. See Scott Raspa, 'A Look at the Top 50 Fintech Companies in Europe', 4 September 2020, <https://finovate.com/a-look-at-the-top-50-fintech-companies-in-europe/>, accessed 15 December 2021.
19. APG, 'APG/MENAFATF Social Media & Terrorism Financing Report', January 2019, p. 6, <http://www.apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142>, accessed 15 December 2021.

1. **Social networking services**: Sites such as Facebook or Twitter, which allow users to create or share social content, as well as connect and interact with other users.
2. **Content hosting services**: Sites which allow users to create, upload and consume content, such as YouTube or Vimeo.
3. **Crowdfunding services**: Sites which – distinct from similar returns-based concerns noted above – allow users to fund a project or cause by soliciting or 'crowdsourcing' small amounts of money from many individuals.[20] Examples include GoFundMe and JustGiving.
4. **Internet communication services**: Also known as instant messaging, which allow users to communicate in real time over the internet, such as WhatsApp or Signal. Increasingly, such services are using end-to-end encryption to prevent surveillance of conversations. Some have even begun to incorporate internet or mobile payment services, such as WeChat Pay.[21]

20. UK Crowdfunding Association, 'What is Crowdfunding?'.
21. WeChat Pay is almost exclusively used in China, though internet communication services platforms operated by Meta (the parent company behind Facebook, Instagram and WhatsApp) now offer payments services in some countries including Brazil, Thailand and the US. See Facebook Pay, 'Current Availability', <https://pay.facebook.com/gb/availability/>, accessed 16 December 2021.

I. Terrorism Financing: Aims and Activities

AS WITH 'NEW technology', the conceptualisation of TF and its real-world manifestations has been similarly imprecise. The UN Security Council's Resolution 2462 (2019) on countering the financing of terrorism denotes the raising, moving, transferring and accessing of funds for and by terrorists as the practical understanding of TF. In contrast, the FATF focuses on the intended use of funds – 'the financing of terrorist acts, and of terrorists and terrorist organisations' – for its definition.[22]

Recent academic literature has helped address this issue by combining both the activities terrorist financiers undertake, and the objectives for which they undertake them, to provide a more comprehensive view of TF. Martin Navias has identified three categories of action (the generation, transfer and use of funds)[23] – an understanding which has recently been clarified further by Jessica Davis, who has provided a consolidated list of six key activities:

- Raising funds.
- Using funds.
- Storing funds.
- Moving funds.
- Managing funds.
- Obscuring funds.[24]

What this more comprehensive approach indicates is that TF is not just about short- to medium-term activities – the raising, using and moving of funds – but also longer-term considerations about the oversight of financial resources.

In addition, researchers have also emphasised the differences between the purposes of operational and organisational financing.[25] In the first instance, operational financing underpins actual or potential attacks, covering preparations, such as research, reconnaissance and

22. See UNSCR 2462 (2019); FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', updated March 2022.
23. Martin S Navias, *Finance & Security: Global Vulnerabilities, Threats and Responses* (London: C Hurst & Co., 2019), p. 49.
24. Jessica Davis, *Illicit Money: Financing Terrorism in the 21st Century* (London: Lynne Rienner, 2021), p. 5.
25. *Ibid.*, pp. 3, 5. See also Colin P Clarke, *Terrorism, Inc.: The Financing of Terrorism, Insurgency, and Irregular Warfare* (Santa Barbara, CA: ABC-CLIO, 2015), p. 4; Nick Ridley, *Terrorist Financing: The Failure of Counter Measures* (Cheltenham: Edward Elgar, 2012).

procurement of weapons or other materials, as well as execution. Organisational financing, by contrast, tends to be more wide-ranging in its objectives, covering the maintenance costs of a terrorist group or network, recruitment and training, the welfare of operatives and sometimes their dependents, the production and dissemination of propaganda, and – occasionally – operational support for wider networks of linked or sympathetic operatives.

This operational/organisational split is an important distinction for understanding the character of TF, as the purpose of funds not only guides the kinds of financial activities that are involved but, at a more granular level, shapes the types of financial tools that might be used. For example, the financing of individual attacks is likely to be less costly, reducing the need to raise, move or use significant funds. This is especially the case in Europe at present, given the prevalence of self-activating terrorism, highlighted by Europol as the chief terrorist threat facing the continent,[26] and constituting 74% of the sample of attacks and plots used in this study. Research suggests that such attackers typically conduct cheaper, self-financed attacks, funded via seemingly licit and banal methods, such as wage income or abuse of state benefits, or via petty criminality like drug trafficking.[27]

By contrast, organisational financing is more likely to require extensive fundraising, much of which will need to be transferred across borders and managed over longer periods of time, putting a particular value on moving, managing, storing – and obfuscating – funds. Hizbullah's European financing operations, for example, have involved front businesses and criminal activities to raise, move and obfuscate funds.[28] Hamas,[29] Al-Shabaab[30] and other Islamist extremist groups have collected donations from Europe-based supporters which are transferred outside of Europe using cash couriers, front companies, bank transfers, money and value transfer services such as MoneyGram and Western Union, and the traditional value transfer system, hawala.[31] Far-right groups domiciled in Europe have done much the same, including groups in Finland and Sweden that raise funds via memberships fees and donations from supporters.[32]

Indirect organisational financing channels are increasingly a TF concern for Europe, whereby funds are transferred to conflict zones but are not intended to financially support the operations

26. Europol, *European Union Terrorism Situation and Trend* (Luxembourg: Publications Office of the EU, 2021), also referred to as 'TE-SAT 2021'.
27. Reimer and Redhead, 'A New Normal'.
28. Matthew Levitt, 'The Lebanese Hizbullah Financing Threat in Europe', Research Briefing No. 1, Project CRAAFT, 2020.
29. US Department of Justice, 'Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts', press release, 13 August 2020, <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>, accessed 9 January 2022.
30. See Magnus Normark and Magnus Ranstorp, 'Understanding Terrorist Finance: Modus Operandi and National CTF-Regimes', Swedish Defence University, 18 December 2015.
31. Europol, 'TE-SAT 2021', p. 33.
32. *Ibid*., p. 31.

of a terrorist group. During the height of the Islamic State's territorial control in Iraq and Syria, the presence of European foreign fighters in the conflict zone prompted friends and family members to transfer funds via informal channels to ensure the wellbeing of their loved ones. The senders of these transfers very rarely shared the ideological views of the recipients, but nonetheless, by providing funds to a terrorist, this has led to several TF convictions in Europe. For instance, in 2019, a British couple was found guilty of TF for sending £233 via a Lebanese intermediary to their Islamic State-supporting son in Syria.[33]

More recently, similar transfers have been made from Switzerland, Sweden, Spain, the Netherlands and other parts of Europe for the purposes of funding foreign fighters' travel back to Europe or supporting individuals detained in camps for Islamic State affiliates, including to pay for human smugglers and facilitators to extract Islamic State-affiliated women and children from such detention facilities.[34] These extraction operations are made possible by complex networks involving Islamic State- and Al-Qa'ida-affiliated terrorist groups such as Hay'at Tahrir al-Sham, who derive profit from an illicit economy in human smuggling.[35]

In sum, as a baseline against which to measure the degree of change in risk posed by new technologies, operational terrorism financing in Europe is dominated by the self-financing of meagre funds by petty criminal and 'banal' means. Organisational financing is, however, more complicated and dependent on fundraising and transferring funds (typically outside of Europe).

Potential Impacts of New Technology on TF

Emerging into this landscape, new technologies have had the potential to disrupt TF conventions, in much the same way that they have disrupted legitimate financial activity. In the literature, and repeated in semi-structured interviews, this idea of new technologies transforming TF has been expressed in three main ways:

- **Offering new channels**: The introduction of a new raft of financial services providers could provide terrorist financiers with new avenues through which to undertake TF. For example, the development of formal crowdfunding platforms and informal social media-based crowdfunding have the potential to provide new ways to move and raise funds.[36]

33. Crown Prosecution Service, 'Sally Lane and John Letts Sentenced for Sending Money to Daesh Supporting Son', <https://www.cps.gov.uk/cps/news/sally-lane-and-john-letts-sentenced-sending-money-daesh-supporting-son>, accessed 9 December 2021.
34. Europol, 'TE-SAT 2021', p. 32.
35. Audrey Alexander, 'Cash Camps: Financing Detainee Activities in Al-Hol and Roj Camps', Combating Terrorism Center at Westpoint, September 2021, pp. 23–27.
36. See Reimer and Redhead, 'Following the Crowd'; Jacobson, 'Terrorist Financing and the Internet'; Martin Rudner, '"Electronic *Jihad*": The Internet as Al Qaeda's Catalyst for Global Terror', *Studies in Conflict and Terrorism* (Vol. 40, No. 1, 2017), pp. 10–23; authors' interview with an EU banking official, 27 August 2021.

- **Supporting TF tradecraft**: VAs, for example, are often taken to be a perfect vehicle for illicit activity, because of their borderless and P2P nature, speed, low transaction costs and supposed anonymity, potentially supporting attack preparation or organisational financing.[37]
- **Reduced surveillance**: Given the relative immaturity of many FinTechs in forming their financial crime controls and becoming familiar with the TF risks they face, it is possible that such platforms might provide a space for terrorist financiers to operate amid weaker financial crime controls than those which exist in the legacy financial sector, where there is greater experience with AML/CTF compliance.[38]

There is a considerable amount of uncertainty and anxiety regarding the extent to which these theoretical risks will or have manifested in reality. In an interview for this project, a senior national law enforcement officer noted that there was a limited understanding of the real nature of the risks among colleagues across Europe, in addition to an underlying concern that they might yet be blindsided by the use of new technology in some unforeseen way.[39] At this point, therefore, this paper turns to the current state of the evidence on the exploitation of new technologies by terrorist financiers in Europe.

37. Zachary K Goldman et al., 'Terrorist Use of Virtual Currencies: Containing the Potential Threat', Center for a New American Security, May 2017; Nikita Malik, *Terror in the Dark: How Terrorists Use Encryption, the Darknet, and Cryptocurrencies* (London: Henry Jackson Society, 2018); Iwa Salami, 'Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?', *Studies in Conflict and Terrorism* (Vol. 41, No. 12, 2017), pp. 968–89; Nicholas Ryder, 'Cryptoassets, Social Media Platforms and Defence Against Terrorism Financing Suspicious Activity Reports: A Step into the Regulatory Unknown', *Journal of Business Law* (Vol. 8, 2020), pp. 668–93. For critical discussions, see Malcolm Campbell-Verduyn, 'Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance', *Crime, Law and Social Change* (Vol. 69, No. 1, 2018); Keatinge, Carlisle and Keen, 'Virtual Currencies and Terrorist Financing'.
38. Authors' interview with senior FinTech financial crime consultant, 7 May 2021; authors' interview with money laundering reporting officer (MLRO) of a European payments provider/FinTech, 28 July 2021; authors' interview with analyst at a European financial intelligence unit (FIU), 13 August 2021; authors' interview with an EU banking official, 27 August 2021; Michael Carter, 'Microlending and Crowdfunding: A Growing Terrorist Financing Risk', *KYC360*, 28 July 2017, <https://www.riskscreen.com/kyc360/article/microlending-and-crowdfunding-aml-risk/>, accessed 22 March 2021.
39. Authors' interview with head of EU member state FIU, 26 July 2021.

II. New Technologies and TF Risk

THE DEBATE ON the TF risks of new technologies has a tendency to polarise around two positions – those that view the perceived vulnerabilities of new technology as a clear and present danger, common among public sector officials,[40] and those that feel that the risks are not necessarily any worse than those posed by the pre-existing financial system, an attitude unsurprisingly more common among those working with new technologies or from academics and researchers with the opportunity to take a longer-term view.[41] This lack of consensus is partly shaped by the roles and interests of those involved, as well as levels of actual exposure to real TF or new technologies. However, it also reflects a lack of consistent evidence, which makes a wider range of divergent assessments possible.

At the most basic level, it is clear that some new technologies are being used for both operational and organisational TF purposes by terrorists of differing ideologies. On the operational side, payment services providers and social media have appeared in a number of cases, while for organisational funding, social media, crowdfunding platforms and VAs have been highlighted as tools for raising and moving funds in both research and the media. However, there is very little evidence to suggest that new technologies have had a transformational effect on TF in Europe thus far. Looked at from a quantitative perspective, TF schemes are still dominated by tried-and-tested methods and, where new technologies do appear, they tend to be used in combination with traditional approaches.

These findings should be caveated, however, with a warning about confidence in the underlying evidence. It was apparent from practitioner interviews – both in the public and private sector – that many felt they had insufficient knowledge to describe the scale and scope of abuse with assurance.[42] This caution points to the need to improve the evidence base on all types of TF, with better categorisation and systematic reporting on TF typologies. This is discussed further in Chapter III.

Operational Financing

The use of new technologies for operational financing gained considerable attention in December 2015, when Syed Rizwan Farook secured a $28,500 loan from P2P lending firm Prosper

40. Authors' interview with head of EU member state FIU, 26 July 2021; authors' interview with EU banking official, 27 August 2021.
41. Authors' interview with MLRO of a European payments provider/FinTech, 28 July 2021.
42. Authors' interview with senior head of an EU member state FIU, 26 July 2021; authors' interview with EU-level officials, 7 June 2021; authors' interview with senior compliance official of major payments services provider, 27 July 2021; authors' interview with head of financial crime compliance at a major payments services provider, 24 July 2021.

Marketplace, just two weeks before he and his wife Tashfeen Malik carried out a politically motivated shooting at a Christmas party in San Bernardino, California. US authorities indicated at the time that the loan may have been used to pay for ammunition, components for several improvised explosive devices and target practice at a gun range.[43]

The San Bernardino example highlights the potential for new technologies to play a role in the raising of funds to support attack preparations. However, it remains a rare example in the US, and based on the open source data-collection exercise for this study, does not reflect the recent situation in Europe either.

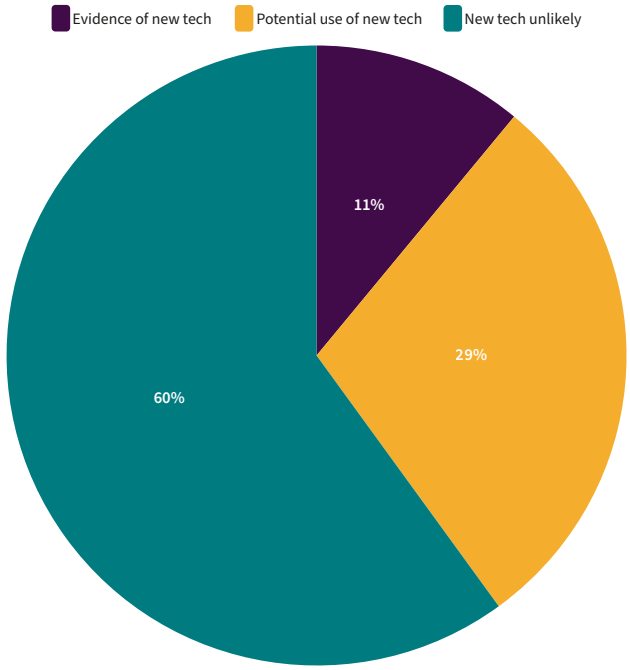
The study included a review of 212 operational cases that have taken place in Europe since January 2015. Useful material on the financial and logistical dimensions of attack planning was found in 65 (31%) of the plots. Although information about the funding and management of these plots was often difficult to fully discern, it was readily apparent that in the majority of cases, new technologies did not feature prominently in operational TF:

- In 60%, it appeared highly unlikely that any new technologies had been used, for a number of reasons: reporting indicated that attack-related items had been previously owned by the attacker; or had been procured using cash or common banking payment methods.
- In 29%, reporting indicated that some form of financial technology had potentially been used to purchase items online or in store, but it was not clear whether this was through legacy banking products, or those provided by a challenger bank or payment services provider.
- In 11%, reporting indicated the likely use of new technologies for operational TF.

These findings are presented visually in Figure 1.

43. James Rufus Koren and Jim Puzzanghera, 'Loan to San Bernardino Shooter Draws Scrutiny to Online Lending Industry', *Los Angeles Times*, 11 December 2015; *BBC News*, 'San Bernardino Shooting: What We Know So Far', 11 December 2015.

Figure 1: Use of New Technologies in Attack Planning in Europe, 2015–21



Source: Based on 65 cases from the authors' research.

In light of the relatively small numbers of cases with explicit evidence of the involvement of new technologies, the paper explores a few cases in greater detail (see Boxes 1 and 2).

Box 1: Dark Net Purchases in Cryptocurrencies

In two instances of new technologies being used to purchase attack components, European self-activating terrorists purchased weapons on the dark net using cryptocurrencies. Ali David Sonboly, a far-right terrorist from Germany who was inspired by Norwegian terrorist Anders Breivik, shot and killed nine people in Munich in 2016. After the attack, a 32-year-old German man was arrested for attempting to sell automatic weapons and a pistol to undercover agents he had met on the dark net. The man later confessed to also selling Sonboly a Glock 17 pistol and 350 rounds of ammunition during two meetings in the city of Marburg. The materials cost Sonboly €4,350, which he paid for in Bitcoin.

Steven Bishop's foiled plot to bomb a south London mosque similarly revealed attempts to purchase IED components on the dark net, including a detonator. Although reporting does not indicate whether this item was purchased with fiat currency or VAs, it is highly likely to have been the latter, given that they are the primary currencies used for the sale of illicit goods on dark net marketplaces. In another instance, Stephan Balliet, the gunman in the Halle synagogue shooting of October 2019, is known to have received a donation in Bitcoin from an undisclosed party prior to his attack, although he made the weapons used with a 3D printer.

Sources: Daniel Koehler, 'The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat', CTC Sentinel *(Vol. 12, No. 11, December 2019); Ruth Bender and Christopher Alessi, 'Munich Shooter Likely Bought Reactivated Pistol on Dark Net',* Wall Street Journal*, updated 24 July 2016; Reuters, 'German Admits Selling Gun to Munich Attack Shooter', 28 August 2017; Kim Sengupta, 'The Dark Web is a Dangerous New Frontier for Those Who Try to Keep Terrorists at Bay',* The Independent*, 26 August 2016; Lizzie Dearden, 'Man Planned to Bomb London Mosque in "Revenge" for Manchester Arena Attack',* The Independent*, 9 April 2019;* Wimbledon Times*, 'Man Arrested at His Mother's Morden Home Plotted to Blow Up Mosque in a Suicide Mission, a Court Heard', 6 November 2018; Sven Röbel, 'Halle-Attentäter wurde von Unbekanntem finanziell unterstützt' ['Halle Assassin was Financially Supported by Unknown Persons'],* Spiegel Panorama*, 11 October 2019.*

Box 2: Online Payments Services

Three instances demonstrate the use of FinTechs offering payment services to purchase attack components. Two cases in the UK involved the use of PayPal accounts to make purchases: Mohammed Rehman, who plotted to attack the London Underground or the Westfield shopping centre on the 10th anniversary of the 7/7 bombings, bought precursor chemicals and other materials on eBay; teenager Haider Ahmed planned an attack using a hunting knife he purchased using PayPal for £25, though his plot was foiled after his mother found and confiscated the weapon.

A 2019 IED attack in Lyon, France was financed using income the attacker had earned from offering private online lessons using Udemy. Revenue from the platform was paid into the attacker's account with Payoneer, a financial services provider specialised in facilitating payments for sellers of goods and services on online marketplaces. IED components purchased on Amazon were paid for using a payment card linked to the Payoneer account. This case stands out as exhibiting particular competence in using new technologies to raise and spend funds for operational activity. The attacker also had three PayPal accounts and cryptocurrency reserves held in an account with Coinmama, a cryptocurrency exchange.

Sources: BBC News*, '"Silent Bomber" Couple Found Guilty of London Terror Attack Plan', 29 December 2015; Peter Stubley, 'Wife of Suspected ISIS Terrorist "Used Payday Loans to Fund His Bomb-Making Purchases on eBay"',* The Mirror*, 2 December 2015;* BBC News*, 'Redhill Man Haider Ahmed Jailed Over Knife Terror Plot', 28 June 2019;* France 24*, 'Lyon Blast Suspect Appears Before Anti-Terror Judge', 31 May 2019; authors' video interview with French officials, July 2020.*

As highlighted by Boxes 1 and 2, it does not appear that new technologies have played a predominant role in the financing of most European terrorist attacks in recent years. Most notably, VAs do not appear to have taken off as a means of procuring weapons. Despite concerns about the anonymity they might provide for dark net purchases, VAs – in the case of the most widely used cryptocurrencies – also provide a publicly available ledger of transactions, which has potentially discouraged its wider use. Indeed, the technological prowess necessary to navigate and successfully make purchases on the dark net with VAs would seem to be beyond the vast majority of terrorists planning their own attacks.[44] The use of payment platforms to procure items does feature, although it is noteworthy that the providers exploited were not necessarily the newest entrants to the market, but more established firms – in particular PayPal. There are also scant indications that terrorists have turned to digital banking en masse, or sought to fund attacks using lending or crowdfunding facilities, along the lines of the San Bernardino case. Nonetheless, with such a large number of cases difficult to code due to lack of information, this judgement should be made with a certain amount of caution.

44. Authors' interview with Kayla Izenman, an asset listing researcher at Coinbase and RUSI Associate Fellow, 14 May 2021.

Organisational Financing

There has been much more conspicuous discussion across the research community and the media about the role new technologies might play in organisational TF. Here, VAs, donation-based crowdfunding, social media and payments services providers have been central, with the typologies most commonly explored being the new platforms' role in raising and moving funds.[45]

There is ample evidence of terrorist groups of various ideological stripes promoting the use of VAs in particular. The Islamic State began to tell supporters to use Bitcoin in 2014, although there are indications that it has more recently switched to encouraging the use of privacy coins such as Monero.[46] Other Islamist extremist groups have also promoted the use of VAs for fundraising, such as the Mujahideen Shura Council in 2016 and Hamas in March 2019.[47] Some extreme right-wing groups in the US and Europe have followed a similar path, with Scandinavian groups such as the Nordic Resistance Movement and Nordic Strength collecting donations online via VAs.[48]

Nonetheless, as with operational financing, caution is required before drawing too many potentially sensational conclusions. For the most discussed technology – VAs – it is unclear how much impact they have actually had. A US government action in August 2020 is reported to have led to the seizure of millions of dollars' worth of Islamist extremist groups' VA assets,[49] but in other instances, it has not been clear that groups have gained much benefit from VA-based fundraising. For example, the aforementioned campaign by the Mujahideen Shura Council was only able to raise the equivalent of $500.[50] Recent analysis by blockchain analytics firms such as Chainalysis has further shown how, despite terrorist groups' use of cryptocurrencies, they are failing to keep it out of the hands of law enforcement agencies, who are becoming adept at tracking and seizing funds.[51]

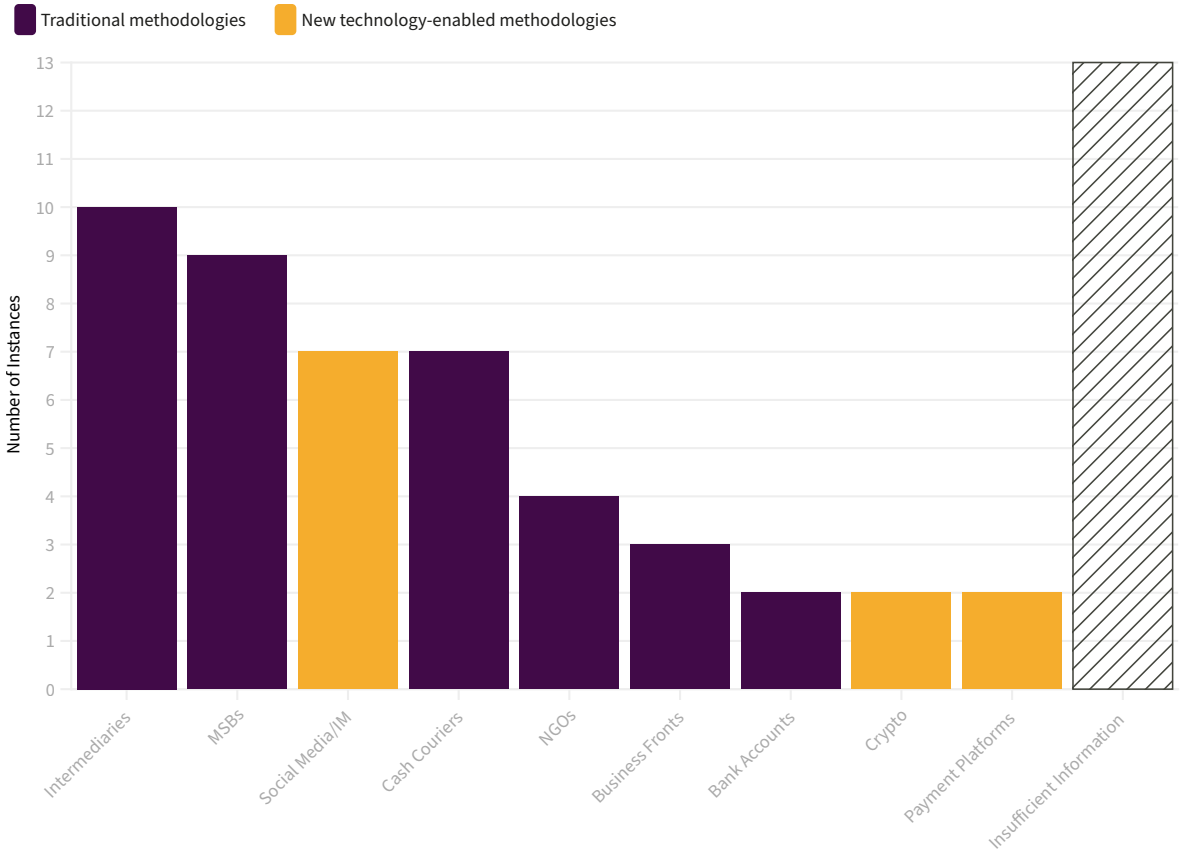
45. See Reimer and Redhead, 'Following the Crowd'.
46. Stan Higgins, 'ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide', CoinDesk, updated 11 September 2021, <https://www.coindesk.com/markets/2014/07/07/isis-linked-blog-bitcoin-can-fund-terrorist-movements-worldwide/>, accessed 9 January 2022; Andrey Shevchenko, 'ISIS-Affiliated News Website to Collect Donations with Monero', CoinTelegraph, 25 June 2020, <https://cointelegraph.com/news/isis-affiliated-news-website-to-collect-donations-with-monero>, accessed 9 January 2022.
47. Antonia Ward, 'Bitcoin and the Dark Web: The New Terrorist Threat?', RAND, 22 January 2018, <https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html>, accessed 9 January 2022; Tom Wilson and Dan Williams, 'Hamas Shifts Tactics in Bitcoin Fundraising, Highlighting Crypto Risks: Research', *Reuters*, 26 April 2019.
48. Europol, 'TE-SAT 2021', p. 31.
49. US Department of Justice, 'Global Disruption of Three Terror Finance Cyber-Enabled Campaigns'.
50. Ted Knutson, 'Terrorists Trying Multiple Times to Raise Funds Via Crypto – Without Much Success, Congress Told', *Forbes*, 7 September 2018.
51. Chainalysis, 'The 2022 Crypto Crime Report', p. 93.

Beyond VAs, two interviewees with an insight into a range of European TF cases noted that other new technologies – especially payment services providers – were appearing with greater regularity in organisational financing schemes. Even then, they assessed that the role of payment platforms was still relatively limited in comparison with the use of the traditional financial system or alternative value transfer systems, such as Islamic banking tools including hawala. As with operational financing cases, moreover, older payment platforms such as PayPal were more likely to appear.[52]

This nuanced perspective was largely borne out in the quantitative analysis of organisational TF cases for this study. Forty-nine cases were identified[53] – mostly involving Islamist extremists seeking to move funds from European countries to destinations in the Middle East and North Africa, often to support foreign fighters or their dependents. Of these 49 cases, 36 included material that was sufficient for drawing conclusions about the TF methodologies used, among which 52 methodologies were identified, with several in combination in one case.

52. Authors' interview with EU-level officials, 7 June 2021.
53. As with the sample of 212 operational cases identified, the sample of 49 organisational financing cases is almost certainly incomplete. It cannot be said how many operational cases have occurred in the period of study but have not been reported. As outlined in the Methodology section, it can be expected that the lag time between an instance of far-right organisational TF and an investigation yielding judicial action (and thus being reported in the media or the other public sector sources used in this study) may contribute to this.

Figure 2: Organisational Terrorism Financing Methodologies Identified in 49 European Cases



Key: purple = 'traditional methodologies'; yellow = 'new technology-enabled methodologies'.

Source: Author generated.

Clearly, 'traditional' means of organisational financing far outstripped those involving new technologies. The top three methodologies mentioned were 'intermediaries' to facilitate or undertake the transfer of funds (10 cases, 20%), money service businesses (MSBs) (nine cases, 18%) and hawala (seven cases, 14%). Cash couriers were also significant (six cases, 12%), and sometimes appeared to be one and the same with the 'intermediaries' mentioned in case reporting.

FinTech featured much less prominently, with cases involving online payments services and cryptocurrencies representing the smallest number of methodologies, although the examples of VA use were relatively recent (see Box 3).

Box 3: Cryptocurrency and Organisational Financing

French law enforcement arrested 29 individuals in September 2020 for financing jihadist groups in Syria using cryptocurrency coupons worth between €10 and €150 purchased from licenced tobacco outlets across France. Paid for with cash or a credit card without having to produce ID, the voucher references were then communicated to contacts in Syria using encrypted messaging, who could use them to credit their own Bitcoin wallets. France announced new know-your-customer (KYC) rules applying to all cryptocurrency providers following the incident.

In the UK, Hisham Chaudhary (convicted in September 2021) received tens of thousands of pounds in funds from Islamic State-linked contacts in 2018, and was tasked with converting funds into cryptocurrency (Bitcoin) and then distributing it onwards for the group's use. It was reported that Chaudhary purchased £17,000 worth of Bitcoin in 2018, of which £16,000 was transferred to unidentified sources. He then bought and transferred around £35,000 via Bitcoin in 2019. The funds were supposedly intended for organising the extraction of Islamic State affiliates from detention camps and their transportation to areas controlled by the Islamic State.

Sources: France 24*, 'France Arrests 29 in Anti-Terror Syria Financing Sting', 29 September 2020; Gabriel Vedrenne, 'Cryptocurrency "Coupons" Funded Syrian Jihadism, French Authorities Claim', Moneylaundering.com, 2 October 2020, <https://www.moneylaundering.com/news/cryptocurrency-coupons-funded-syrian-jihadism-french-authorities-claim/>, accessed 18 December 2021; Vish Gain, 'France Announces Strict Cryptocurrency KYC Rules to Fight Money Laundering and Terrorist Financing', AML Intelligence, 11 December 2020, <https://www.amlintelligence.com/2020/12/france-announces-strict-cryptocurrency-kyc-rules-to-fight-money-laundering-and-terrorist-financing/>, accessed 18 December 2021;* BBC News*, 'Hisham Chaudhary: Oadby Terrorist Who Funded IS with Bitcoin Jailed', 3 September 2021.*

Nonetheless, despite the relatively small role of FinTech 'proper', it is important to note that social media was more common, detected in seven instances where extremists shared information to allow funding to be raised or moved, a methodology which has already been well-documented beyond Europe.[54] In attempts to disguise their activities, terrorist financiers claim to be collecting funds for legitimate charitable or humanitarian activities when soliciting donations via social media,[55] an approach used in Spain in 2021, when three individuals diverted funds collected for a non-profit organisation to finance the activities of Al-Qa'ida.[56] In such cases, the resultant donations are then typically made using traditional payment methods such as bank transfers,[57] although there are instances of pre-paid cards and cryptocurrencies being used.[58]

These cases indicate the important role internet-enabled technologies can play in the raising and managing of funds in organisational TF,[59] and how easily they dovetail with other approaches. An unnamed defendant in Sweden, tried for terrorist offences in February 2017, used Facebook to post bank account details for known terrorists.[60] In a further example, Mohammed Iqbal Golamaully and Nazimabee Golamaully, convicted in London in November 2016, sent funds to their nephew Zaffir in Syria via a courier, although they made arrangements for sending the funds via WhatsApp. Another case combining social media and other techniques is outlined in Box 4.

54. Jessica Davis, 'New Technologies but Old Methods in Terrorism Financing', Research Briefing No. 2, Project CRAAFT, 2020.
55. Rudner, '"Electronic *Jihad*"'.
56. Europol, 'Three Arrested in Spain for Terrorist Financing', 26 March 2021, <https://www.europol.europa.eu/media-press/newsroom/news/three-arrested-in-spain-for-terrorist-financing>, accessed 18 December 2021.
57. APG/MENAFATF, 'Social Media and Terrorism Financing', 2019, <http://www.apgml.org/news/details.aspx?n=1142>, accessed 14 January 2022.
58. FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)', February 2015, pp. 24–25; US Department of Justice, 'Global Disruption of Three Terror Finance Cyber-Enabled Campaigns'.
59. Jacobson, 'Terrorist Financing and the Internet'; UN Office on Drugs and Crime (UNODC), 'The Use of the Internet for Terrorist Purposes', 2012, <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>, accessed 19 March 2021.
60. Eurojust, 'Terrorism Convictions Monitor' (No. 30, April 2018), p. 24, <https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2018-04_TCM-30_EN.pdf>, accessed 14 January 2021.

Box 4: 'Justice for Sisters': Online Crowdfunding and Indirect Organisational Financing

The so-called 'Justice for Sisters' campaign in summer 2019 demonstrated Islamist extremist tendencies to use the cover of humanitarian action to collect funds prior to cross-border transmission. The campaign raised thousands of euros via online 'pop-up' crowdfunding on social media, ostensibly for female detainees at the Al-Hol camp in northern Syria.

Campaigners disseminated videos, pictures and written accounts in German, English and Arabic on Telegram channels associated with the Islamic State, often evoking the welfare of their young children to coax donations. Donors were then directed to several PayPal MoneyPool accounts, which were kept below €1,800 (the threshold above which the holder of the account is asked for additional identifying information to aid due diligence, in accordance with European law). Funds were then allegedly transferred from a German intermediary to Turkey via hawala transfers, moving it to shopkeepers inside the camp in Syria. To evade detection by PayPal, donors were instructed to avoid using Islamic terms in their payment references, with campaigns labelled as 'Honeymoon in Vienna', among other phrases.

Sources: Richard Hall, 'ISIS Suspects in Syrian Camp Raise Thousands Through Online Crowdfunding Campaign', The Independent*, 25 July 2019; Afshin Ismaeli and Hanne Christiansen, 'IS-kvinner samler inn penger til «bryllupsreise til Wien». Målet er å unngå straffeforfølgelse i Europa' ['ISIS Women Raise Money for "Honeymoon to Vienna". The Aim Is to Avoid Prosecution in Europe'],* Aftenposten*, 4 August 2019, <https://www.aftenposten.no/verden/i/wP4J71/is-kvinner-samler-inn-penger-til-bryllupsreise-til-wien-maalet-er-aa>, accessed 29 June 2021.*

A further, emerging TF typology involving social media involves terrorist groups and individual extremists generating advertising revenue from content hosting services. Tom Keatinge and Florence Keen have highlighted how posting terrorist content can earn revenue by having brand advertisements appear on their videos.[61] One such example was uncovered in 2017, when brands including Mercedes Benz and the UK supermarket chain Waitrose had their advertisements appear on posts by the Islamic State.[62] This fundraising strategy has also been adopted by the far right, who are able to monetise extremist ideology dissemination on platforms such as Instagram, TikTok, YouTube, Twitch and DLive.[63]

61. Tom Keatinge and Florence Keen, 'Social Media and Terrorist Financing: What Are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?', Global Research Network on Terrorism and Technology, Paper No. 10, RUSI, 2019, <https://static.rusi.org/20190802_grntt_paper_10.pdf>, accessed 31 January 2022.
62. Alexi Mostrous, 'Big Brands Fund Terror Through Online Adverts', *The Times*, 9 February 2017.
63. US House of Representatives Committee on Financial Services, 'Memorandum: February 25, 2021, NSIDMP Hearing Entitled, "Dollars Against Democracy: Domestic Terrorist Financing in the Aftermath of the Insurrection"', 22 February 2021, <https://financialservices.house.gov/uploadedfiles/hhrg-117-ba10-20210225-sd002.pdf>, accessed 18 March 2021; Megan Squire, 'Monetizing Propaganda: How Far-Right Extremists Earn Money by Video Streaming', conference

Assessment

Based on the data collected, it appears that the majority of sub-sectors of FinTech have not featured in operational or organisational TF in Europe since 2015. Evidence for their use is largely absent from what is publicly known about attack planning, although payment services providers do appear in a number of cases, and – along with digital banks – might appear in more, if more case material were available. Older payments platforms and VAs have played a slightly more visible role in the organisational financing of Islamist extremists in the period under study, but traditional means – couriers, intermediaries, MSBs and hawala – still formed the backbone of organisational fund raising and flows. More important, however, has been social media, which has played promotional and organisational roles in the raising and management of funds, sometimes in combination with the 'core' conventional methodologies. As Davis has noted, new technologies are more likely to appear in the context of pre-existing methods of TF, rather than as transformational tools in their own right.[64]

These findings pose two important questions:

1. Why are terrorists not making more use of FinTech, especially newer providers, at the moment?
2. How likely is it that unseen evidence could force a different conclusion?

On the first question, it seems unlikely that the self-activating terrorists operating in Europe need to innovate financially to execute some of the low-complexity attacks they are currently undertaking. Knives, blunt instruments and many parts of IEDs or incendiary devices can be bought easily on the surface internet (or in shops) using pre-existing traditional back accounts and/or first generation FinTech such as PayPal.[65] For organisational financiers, the same might also be true, especially among Islamist extremists, who have tried and tested payment mechanisms such as hawala that are difficult to monitor.

Previous work in the area has indeed underlined that there are good reasons why we would not see a major shift in approach because of the nature of terrorist decision-making. A behavioural finance study by Peter J Phillips and Benjamin McDermid suggests there are good grounds to believe that the decisions of terrorist financiers will be 'sticky', and systematically biased in favour of older, more familiar and – importantly – previously reliable modes of funds transfer.[66] In a further study, Tom Keatinge and Kerstin Danner find that terrorist financial innovation is

paper, WebSci '21: 13th International ACM Conference on Web Science in 2021, <https://drive.google.com/file/d/1Sg2TJsi7G1QJ-QtuCl5y-u6nim32JwfY/view>, accessed 31 January 2022.

64. Davis, 'New Technologies but Old Methods in Terrorism Financing'.
65. See Reimer and Redhead, 'A New Normal'.
66. Peter J Phillips and Benjamin McDermid, 'FinTech, Terrorism-Related Fund Transfers and Behavioural Finance', *Dynamics of Asymmetric Conflict* (Vol. 14, No. 3, 2021), pp. 226–46.

most often driven by necessity 'and in reaction to external forces'.[67] In other words, if the past approaches still seem to work, then there is less incentive to fix them.

There are also other potential reasons to consider with regard to the difficulties of making a shift towards using new technologies. As noted in the previous chapter, there can be a presumption that FinTech is more vulnerable to terrorists and other criminals because of lower due diligence standards. However, while accepting that many new FinTechs are likely to be highly vulnerable at an early stage of growth, when systems and procedures are new, this will not last forever. A money laundering reporting officer (MLRO) at a major FinTech firm interviewed for this research, who had previously worked within the legacy financial sector, did not believe that there was a material difference in the standards between 'old' and 'new' tech after a certain point in the 'maturity curve' had been reached. The head of a global compliance consultancy which worked closely with FinTech firms took a similar view.[68] In sum, established FinTechs are not necessarily any more hospitable to terrorists than conventional financial institutions.

Finally, there is the issue of difficulty of use and accessibility, which affects VAs in particular. Using VAs to buy items for an attack on the surface internet is still difficult, and the use of the dark net takes additional technical skill – and confidence. Nikita Malik has also previously noted that the assumed anonymity afforded to users of cryptocurrencies is not guaranteed, given that a publicly accessible blockchain of cryptocurrency transactions permits those with sufficient computer literacy to 'trace the digital footprint of anonymous traders'.[69] Tom Keatinge, David Carlisle and Florence Keen have also highlighted the difficulty of using VAs for organisational TF purposes because of the difficulty in converting them back into fiat currency for use in the conventional economy.[70] It is likely for these reasons that the UK's 2020 national risk assessment, for example, notes that while there is a small growth in terrorist use of VAs,[71] it is highly unlikely that usage is widespread.[72]

The second question is obviously much more challenging. It seems unlikely that many sectors of FinTech are being exploited on a large scale, but there are still reasons to keep a close watch on

67. Tom Keatinge and Kerstin Danner, 'Assessing Innovation in Terrorist Financing', *Studies in Conflict and Terrorism* (Vol. 44, No. 6, 2021), pp. 455–72.
68. Authors' interview with MLRO of a FinTech offering payments services, 27 May 2021; authors' interview with senior FinTech financial crime consultant, 7 May 2021.
69. Malik, *Terror in the Dark*.
70. Keatinge, Carlisle and Keen, 'Virtual Currencies and Terrorist Financing'; Salami, 'Terrorism Financing with Virtual Currencies'.
71. The risk rating for VAs was increased from low to medium for TF between 2017 and 2020, citing increasing accessibility on the back of improvements in VA technology.
72. See HM Treasury and Home Office, *National Risk Assessment of Money Laundering and Terrorist Financing 2020* (London: The Stationery Office, 2020).

those 'volume' providers involved in the use and transmission of funds, especially in the digital banking and payments services subsectors.[73] A further area for caution is the scale of past VA exploitation. According to evidence presented at his trial, Hisham Chaudhary commented to associates on Telegram that the Islamic State had been using cryptocurrency 'for years' to conduct organisational financing.[74] A throwaway line perhaps, but one that should be explored further. As the following exploration of current CTF responses demonstrates, more comprehensive data collection will be essential to taking a more sensitive and pertinent approach to the real risks in FinTech.

73. Authors' interview with head of financial crime compliance at a major payments services provider, 24 July 2021.
74. James Rodger, 'Sales Consultant with "Saviour Complex" Jailed for Funding ISIS with Bitcoin', *Birmingham Mail*, 3 September 2021.

III. Current Responses

THE ROLE OF new technology in TF was highlighted by the FATF in October 2015 in its report on 'Emerging Terrorist Financing Risks', alongside 'traditional' issues such as the use of MSBs, cash couriers and hawala.[75] Since then, the topic has engaged key stakeholders in the EU's CTF estate. Policymakers have updated regulations around VAs and crowdfunding, and established elements of the financial sector have sought to limit risks by reducing exposure to some FinTech clients, especially VASPs.

However, as seen in Chapter II, the risks faced across different elements within the FinTech sector vary widely and are, on current evidence, likely more negligible than many fear. In some ways, VAs have become the bogey man of the FinTech sector, and the 'go to' point of discussion of where emerging TF risks lie, in conversation with officials and compliance experts.[76] Yet, this is probably an over-estimation of the importance of VAs within FinTech as a whole, and also of TF risk at present. Digital banking and payment services providers represent larger parts of the FinTech market, and – even though also apparently not subject to high TF risks – might be of more concern with a better evidence base. In addition, the current EU approach does not take into account issues around social media – a new technology which is not 'FinTech' as such, but where there are already perceptible TF dangers which have not been adequately addressed.

This chapter will assess the state of the current response to perceived TF abuses of new technologies, with a view to determining the overall risk posed. If, for instance, the mitigating measures and responses currently employed are adequate and proportional to the state of the threat, as outlined in Chapter II, then the degree to which existing risk has been changed by the advent of new technologies would be limited. Responses by the public and private sectors will be appraised.

The EU and CTF

Following the FATF guidelines, the EU's regulatory approach to CTF is fully integrated into its AML framework, and is outlined in six successive versions of the EU's Anti-Money Laundering Directive (AMLD), the most recent issued in October 2018. Each version provides a set of minimum standards for member states to meet, although the European Commission's new

75. FATF, 'Emerging Terrorist Financing Risks', October 2015, pp. 30–39.
76. Authors' interview with senior head of EU member state FIU, 26 July 2021; authors' interview with EU-level officials, 7 June 2021; authors' interview with senior FinTech financial crime consultant, 7 May 2021.

AML plan, issued in July 2021, seeks to create a consistent and unitary approach across all member states.[77]

Although the requirements of the AMLDs have become broader and more detailed over time, the core elements have remained largely the same. TF offences have been criminalised, and the private sector obligated to act as gatekeepers of the financial system. Firms within and operating on the edges of the financial sector thus need to undertake varying grades of customer due diligence (CDD) to identify potential known terrorist financiers and monitor client behaviour to detect unusual activities that might be linked to TF. In the event that these appear suspicious, obligated entities must report these cases as suspicious transaction reports (STRs) to a national FIU for further sharing with law enforcement or other competent authorities.[78]

As well as the regulatory foundation, the EU has a range of institutions with some competence in the AML/CTF space. From the supervisory perspective, three European Supervisory Authorities (ESAs), of which the most significant is the European Banking Authority (EBA),[79] have held a brief to support supervisory information sharing on AML/CTF. The policing agency, Europol, also plays an important role as an intelligence hub on CTF, housing the European Counter-Terrorism Centre (ECTC), the European end of the EU–US Terrorist Finance Tracking Program (TFTP), and the European Financial Intelligence Public/Private Partnership (EFIPPP), which includes national law enforcement agencies, regulators and significant financial institutions in strategic intelligence sharing across all predicate AML/CTF offences.[80]

Handling TF and New Technologies

Policymakers within the EU have targeted VAs and VASPs as the riskiest new financial technologies with regard to TF.[81] Those framing the language of the Commission's new AML/CTF plan have targeted the emergence of VAs as one of the chief reasons why reform is necessary. In announcing new measures on 20 July 2021, the Commission noted that it was reforming the system in order to take 'into account new and emerging challenges linked to technological innovation',

77. European Commission, 'Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)', 20 July 2021, <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_3689>, accessed 10 December 2021.
78. See Matthew Redhead, 'Deep Impact? Refocusing the Anti-Money Laundering Model on Evidence and Outcomes', *RUSI Occasional Papers* (October 2019).
79. Of which the other two are the European Insurance and Occupational Pension Authority (EIOPA) and the European Securities and Market Authority (ESMA).
80. RUSI, 'Survey Report: Five Years of Growth in Public–Private Financial Information-Sharing Partnerships to Tackle Crime', August 2020, pp. 79–81, <https://www.future-fis.com/uploads/3/7/9/4/3794525/five_years_of_growth_of_public-private_partnerships_to_fight_financial_crime_-_18_aug_2020.pdf>, accessed 13 December 2021.
81. Authors' interview with European banking official, 27 August 2021.

specifically calling out 'virtual currencies'.[82] Unsurprisingly, there has been a consistent EU push to ensure that a wider array of VASPs are covered by the AML/CTF regime. This started with the inclusion of VASPs that stand at the edge of the fiat/VA world, such as fiat-to-cryptocurrency exchanges, and custodian wallets, in the fifth AMLD in May 2018,[83] and has now proposed it cover all other types of VASP, including VA-to-VA exchanges, under the new AML plan.[84] The Commission has further proposed extending the 2015 Regulation on Transfer of Funds to cover VASPs, to follow new requirements issued by the FATF in June 2019.[85] Known as the 'Travel Rule' within the financial services industry, the change will require all VASPs to collect originator and beneficiary information for any transaction, reducing levels of anonymity for VA users within the EU and for their immediate counter-parties, potentially outside the EU.[86]

At the same time as the push to mitigate potential risks around VAs, elements within the EU machinery have recognised that the challenges new technology might pose for CTF are wider than VAs. However, the potential TF risks from other FinTech sectors have been more quietly accommodated within the pre-existing AML/CTF structures. As most mainstream FinTech subsectors provide services which replicate those of the traditional financial sector, they are arguably subject to AML/CTF requirements by default, although internet-based payments services providers were specifically included in the fourth AMLD in May 2015.[87]

There have been exceptions, with crowdfunding treated as a separate case so far. France passed Ordinance 2014-559 in May 2014, focused on the registration and basic regulation of crowdfunding platforms involved in investments and loans,[88] but it was not widely followed by

82. European Commission, 'Beating Financial Crime: Commission Overhauls Anti-Money Laundering and Countering the Financing of Terrorism Rules', 20 July 2021, <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3690>, accessed 20 December 2021.
83. *Official Journal of the European Union*, 'Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU', 19 June 2018, p. 2, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN>, accessed 13 December 2021.
84. European Commission, 'Beating Financial Crime'.
85. FATF, 'Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers', October 2021.
86. This follows changes required by the FATF. See *ibid.*
87. *Official Journal of the European Union*, 'Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC', 5 June 2015, p. 2, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN>, accessed 13 December 2021.
88. Government of France, 'Ordonnance n° 2014-559 du 30 mai 2014 relative au financement participatif', <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029008408/>, accessed

other EU states. The EU issued its own Crowdfunding Regulation for return-based platforms in October 2020, introducing the requirement to conduct CDD on those seeking funding, although not explicitly for AML/CTF reasons.[89] As part of its new AML plan, the Commission is also now recommending the inclusion of donation-based crowdfunding platforms as obligated entities under AML/CTF rules. Profit-based approaches are not included because, in the Commission's assessment, the pre-existing Crowdfunding Regulation 'contains sufficient safeguards for crowdfunding services providers falling under its scope'.[90]

One further area of note is the EU's response to social media. The EU's approach to terrorist content online has involved operational intelligence sharing to facilitate take-downs. However, the EU is now seeking to strengthen this further, with additional legislative requirements that echo the Network Enforcement Act (*Netzwerkdurchsetzungsgesetz* (NetzDG)), passed in Germany in September 2017, which required social media providers to remove terrorist-related content on their platforms.[91] According to the EU's new Regulation Addressing the Dissemination of Terrorist Content Online, issued in May 2021, hosting service providers (HSPs) – those firms that provide the online infrastructure for social media and other websites – will need to identify and take down content 'that incites or solicits someone to commit, or to contribute to the commission of, terrorist offences'.[92] However, although a broad interpretation of the rule might include information shared for TF purposes, it does not make this possibility explicit.

Calibrating Regulations

While the EU cannot be faulted for seeking to address the potential TF risks from new technologies, its policy response has not been nuanced. The EU's approach has been to integrate most elements within the FinTech sector into the pre-existing AML/CTF regulatory framework by default or, in the case of online payments and VAs, by specific addition. This does, of course, have clear benefits: seeking comprehensive coverage of emerging FinTechs could reduce the risk that terrorist financiers will translate their activities into the sector at scale. Nonetheless, given the relative immaturity of much of that sector, and the EU's stated desire to encourage

13 December 2021.

89. *Official Journal of the European Union*, 'Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European Crowdfunding Service Providers for Business, and Amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937', 20 October 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R1503&rid=4>, accessed 21 December 2021.
90. *Ibid.*
91. Ministry of Justice of Germany, 'Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)', <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>, accessed 13 December 2021.
92. EU Monitor, 'Regulation 2021/784 – Addressing the Dissemination of Terrorist Content Online', <https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vlivmgatiaxg>, accessed 10 December 2021.

its growth,[93] imposing the whole regime could be seen as counter-productive. It would have been more appropriate to take a more calibrated response to the risks within each sub-sector, rather than expecting the implementation of standard AML/CTF compliance procedures. In some cases – such as lower risk areas like insurance or investments, for example – this might have pointed towards a lighter-touch approach, whereas in others – such as new payments services providers – it might have required more rigorous compliance measures focused on TF risks.[94] This more granular strategy has been followed in one sub-sector of the FinTech world – crowdfunding – with low-risk return-based platforms being kept out of the AML/CTF regime, and those collecting donations, where risks are greater, being included.[95]

Of course, the rejoinder to granularity is the 'risk-based approach' (RBA). For nearly 20 years, the FATF and its members have said that firms should apply CDD and other measures with sensitivity, to ensure firm-specific risks are identified and internal policies, procedures and controls calibrated accordingly.[96] This is good advice in theory. However, it remains difficult to accomplish, especially when firms are immature and lacking established in-house compliance expertise – an almost universal problem for early years FinTechs.[97] It is, moreover, one that favours those providers where TF risks are likely to be more limited and hamper those where they are likely to be higher. If those sectors who are more at risk are to handle these challenges effectively, there are grounds for more detailed regulatory guidance on CTF (and possibly other anti-financial crime measures) for FinTechs at early stages.

But the most troubling regulatory omission within the EU CTF regime at present is the position of social media. According to the findings of this study, it is one of the more concerning new technologies being used for organisational TF. Yet, it has no CTF obligations under the AMLD, or under a conservative interpretation of the terrorist content regulation. There is clearly a need for this to change, even if such changes do not include being fully obligated under the AML/CTF framework. As previous research conducted by RUSI has suggested, requiring changes to social media platforms' terms of service to broaden definitions of 'terrorist content' is not a difficult request to make.[98] Moreover, requiring social media sites or those hosting them to search for, identify and report the suspicious sharing of financial information, as well as propaganda, would seem a sensible next step, even if it does blur the lines of sectoral obligations. As a European CT expert has noted, terrorists tend not to worry about acting within the boundaries of official

93. European Commission, 'Digital Finance', <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/digital-finance_en>, accessed 22 December 2021.
94. Authors' interview with senior FinTech financial crime consultant, 7 May 2021.
95. Reimer and Redhead, 'Following the Crowd'.
96. FATF, 'Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures', June 2007.
97. Authors' interview with senior FinTech financial crime consultant, 7 May 2021.
98. Keatinge and Keen, 'Social Media and Terrorist Financing', p. 17.

categories, taking 'what is available to hand, and use it in a way that suits them'.[99] Authorities need to demonstrate the same agility if they are to get ahead of the terrorists. However, any such obligation will bring with it other challenges, as content moderation is as fraught with the risk of misidentifying 'false positives' and missing 'false negatives' as transaction monitoring within financial institutions. Developing a set of optimal rules for TF moderation is not an easy task for the private sector, and is another reason why effective application of content moderation calls for better collaboration between the public and private sectors on what platforms should be looking for.[100]

Evaluating Public Sector Effectiveness

There are deeper issues to evaluating the EU's CTF response to new technologies. Much of the proceeding discussion is based on the assumption that the EU is integrating FinTechs and other sectors into a largely effective AML/CTF regime. But this assumption is open to challenge. The model relies on private sector entities being able to identify suitable financial intelligence about TF and supply it to authorities in STRs. However, research indicates this system provides very little intelligence of value, and is bureaucratic and untimely in delivery.[101]

Like many national governments, the EU has sought to remedy this issue with the introduction of a financial intelligence sharing partnership (FISP), the EFIPPP, to create closer strategic communication between the public and private sectors. This has been a positive albeit tentative development. So far, private sector representation at the EFIPPP has been dominated by traditional financial institutions with cross-border interests. If the partnership is to get a better view of real risks in the FinTech and social media sectors, it should be seeking to involve them more closely in the partnership, whether through associate memberships or involvement in working groups. In light of the still fragmentary state of available intelligence on TF risk within these sectors, and the grave concerns among EU policymakers with regard to technologies such as VAs, it would appear it essential to have them present.

Private Sector Reactions

By allowing public sector responses to the abuse of new technologies for TF to be driven by concern for theoretical vulnerabilities, private sector firms have been left, for the most part, to formulate an independent response to the perceived risk, about which they have received little official guidance. These responses can be motivated by the need to fulfil obligations and manage real concerns, but also by anxieties about regulatory and reputational risk.

99. Authors' interview with European academic CT expert, 9 June 2021.
100. Keatinge and Keen, 'Social Media and Terrorist Financing', pp. 15–16.
101. Matthew Redhead, 'The Future of Transaction Monitoring: Better Ways to Detect and Disrupt Financial Crime', SWIFT Institute Working Paper No. 2020-001, January 2020, pp. 5–8.

Although some legacy financial institutions have sought to embrace the potential of FinTech by developing partnerships with new firms or their own 'spin-off' FinTech products,[102] there have been various concerns across the traditional industry about the risks the new firms might bring. Again, VAs have been a particular anxiety, with established banks reluctant to bank cryptocurrency exchanges or facilitate their customers' transactions, typically evoking financial crime concerns as one justification.[103] Rather than manage the uncertain risks of the relationship, some traditional firms have simply decided to avoid them all together.

In the US, where there have been growing concerns about the rise of the far right, there is evidence of some FinTech firms themselves taking the 'de-risking/avoidance' strategy common among older firms. Many fundraising campaigns from far-right groups were de-platformed from mainstream crowdfunding services such as GoFundMe and Kickstarter following the 2017 'Unite the Right' rally in Charlottesville, Virginia. Major payment services providers including PayPal, Stripe, Apple Pay and Google Pay also refused to accept payments on the bespoke crowdfunding platforms set up in response to de-platforming, such as Hatreon and MakerSupport.[104] Payment providers including PayPal also withdrew their services from GiveSendGo following the US Capitol riot on 6 January 2021.[105]

In Europe, however, there appears to have been a less forward-leaning approach so far. Almost all of the FinTech firms and experts in the field interviewed for this research noted how seriously firms were taking AML/CTF compliance; however, they also admitted that many FinTech firms did not see TF as an issue of equal order of concern as fraud or money laundering. As a result, basic TF risks around payments to high-risk jurisdictions would be used in transaction monitoring scenarios, but more sophisticated scenarios would not be developed.[106] In addition, some firms facing difficult TF risks saw these as just being part of the overall risk of doing business. One P2P lender interviewed for this research provided crowdfunded capital to lending companies based

102. *Finextra*, 'UK Banks Plan to Grow Partnerships with Fintech Firms in Wake of Pandemic', 11 October 2021, <https://www.finextra.com/newsarticle/38992/uk-banks-plan-to-grow-partnerships-with-fintech-firms-in-wake-of-pandemic>, accessed 12 January 2022.
103. Lily Russell-Jones, 'HSBC Bans UK Customers From Making Payments to Binance', *City AM*, 4 August 2021.
104. Sheila Dang, 'No Cash for Hate, Say Mainstream Crowdfunding Firms', *Reuters*, 14 August 2017; Vanessa Romo, 'Charlottesville Jury Convicts "Unite the Right" Protester Who Killed Woman', *NPR*, 7 December 2018; Tom Keatinge, Florence Keen and Kayla Izenman, 'Fundraising for Right-Wing Extremist Movements: How They Raise Funds and How to Counter It', *RUSI Journal* (Vol. 164, No. 2, 2019), pp. 10–23.
105. Olivia Solon and Leticia Miranda, '"Too Little, Too Late": Extremism Experts Criticize Payment Companies', *NBC News*, 13 January 2021.
106. Authors' interview with MLRO of banking services FinTech, 22 July 2021; authors' interview with MLRO of a European payments provider/FinTech, 28 July 2021; authors' interview with financial crime head of virtual assets service provider (VASP), 26 July 2021; authors' interview with head of financial crime compliance at a major payments services provider, 24 July 2021; authors' interview with payments-as-a-service (PaaS) FinTech, 23 July 2021.

outside of Europe, who in turn offered payday, car or business loans to individuals. Although the European-based P2P lender could do CDD on the foreign lending company, it was compelled to trust that they were doing the same on the eventual recipients.[107]

However, some FinTech firms are also clearly seeking to take more innovative approaches to handling their TF risks, going beyond the standard AML/CTF model. Being digitally native, and thus not encumbered by the layering of antiquated systems, has enabled some firms to gather data on client behaviour that traditional FIs do not easily collate or track, such as IP addresses and geo-location. With this information, firms will update evaluations of client TF risk based on those behaviours dynamically. If a client logs in frequently from a location different from their stated residence, for example, this could raise a TF red flag.[108] Similarly, some established FinTech firms have invested resources in network analysis tools, allowing them to do proactive CTF analysis, including screening customer lists for potential associates (recipients of transfers) of terrorists identified by law enforcement.[109] The analysis of social media intelligence (SOCMINT) is already integrated into the financial crime risk management of many FinTech firms.[110] There is also a strong appetite among FinTech firms to contribute to the workings of FISPs. Those that are easiest to join are private–private endeavours such as the global FinTech Financial Crime Exchange (FFE), which has many European members,[111] and encourages the proactive sharing of typological information on TF and other financial crimes. However, although several FinTech firms interviewed for this research indicated their strong interest in joining state-led public–private FISPs, in their jurisdictions, many had found them to be 'closed shops' that favoured working between law enforcement and large, legacy financial institutions.[112]

What of social media? Content moderation has been turbocharged following the far-right attack in Christchurch, New Zealand of 2019, which the perpetrator recorded and livestreamed on social media platforms. In response, the Christchurch Call – issued by the governments of New Zealand and France – sought to encourage technology companies to work with governments to eliminate terrorist content online, building on already established private–private cooperation,[113] radicalisation-focused research programmes funded by social media companies

107. Authors' interview with the compliance team of a European P2P lending platform, 28 May 2021.
108. Authors' interview with MLRO of a major FinTech offering payments services, 27 May 2021.
109. *Ibid.*
110. Tom Keatinge and Florence Keen, 'Social Media and Terrorist Financing: Time for a Focused Response', *RUSI Newsbrief* (Vol. 37, No. 4, October 2017); Tom Keatinge and Florence Keen, 'Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool', *Studies in Conflict and Terrorism* (Vol. 42, No. 1–2, 2019), pp. 178–205.
111. FINTRAIL, 'FinTech FinCrime Exchange', <https://fintrail.com/ffe>, accessed 16 March 2022.
112. Authors' interview with head of financial crime compliance at a major payments services provider, 24 July 2021; authors' interview with MLRO of a major FinTech offering payments services, 27 May 2021; authors' interview with MLRO of banking services FinTech, 22 July 2021.
113. The Global Internet Forum to Counter Terrorism (GIFCT) was established in 2017 by Facebook, Microsoft, Twitter and YouTube 'to prevent terrorists and violent extremists from exploiting digital platforms [by] foster[ing] technical collaboration among member companies, advanc[ing] relevant

themselves,[114] and the use of content moderators and automated content removal systems. However, these initiatives have rarely focused on the problems of social media being exploited for TF purposes.[115]

Social media sites like Facebook have taken matters into their own hands when faced with non-designated yet unpalatable extremists using their platform, including for financing purposes. Its Dangerous Individuals and Organizations policy dictates what users are allowed to say about a self-populated list of 'organizations with a record of terrorist or violent criminal activity'.[116] Alongside a leaked snapshot of the list itself,[117] which includes plenty of Islamist extremist and far-right entities not on any terrorism designation list, guidelines for content moderators were published by The Intercept in October 2021, which require the removal of posts 'providing direct (fundraising, donation-drive, etc.) or indirect (money laundering, accounting or banking services, etc.) financial support to an organization [on the list]'.[118] How widespread this approach has become across all social media sites is not, as yet, apparent.

Assessing the Private Sector Response

Different elements within the legacy financial sector, FinTech and social media sectors have taken three broadly divergent responses to the management of TF risks: avoid the risks through non-engagement; de-prioritise those risks within pre-existing compliance frameworks; or seek to manage those risks more proactively with new tools and external engagement.

Within the context of the relatively low to moderate TF risks from most FinTech sectors that this study has suggested, it would seem that a blanket rejectionist response would be an over-reaction, even for controversial sub-sectors such as VASPs. Such de-risking choices might

research, and shar[ing] knowledge with smaller platforms'. See GIFCT, 'About', <https://gifct.org/about/>, accessed 18 March 2021. The same year, Tech Against Terrorism was set up by the UN's Counter Terrorism Executive Directorate with a similar mandate.

114. The Global Network on Extremism and Technology is the academic research arm of GIFCT run out of the International Centre for the Study of Radicalisation at King's College London.
115. Tech Against Terrorism hosted a rare CTF-focused event in October 2021. See Tech Against Terrorism, 'TAT & GIFCT E-Learning Session – Online Terrorist Financing: Assessing the Risks and Mitigation Strategies', <https://www.techagainstterrorism.org/event/tat-gifct-e-learning-session-online-terrorist-financing-assessing-the-risks-and-mitigation-strategies/>, accessed 14 January 2022.
116. Sam Biddle, 'Revealed: Facebook's Secret Blacklist of "Dangerous Individuals and Organizations"', *The Intercept*, 12 October 2021.
117. *The Intercept*, 'Facebook Dangerous Individuals and Organizations List (Reproduced Snapshot)', 12 October 2021, <https://theintercept.com/document/2021/10/12/facebook-dangerous-individuals-and-organizations-list-reproduced-snapshot/>, accessed 7 January 2022.
118. *The Intercept*, 'Facebook Praise, Support and Representation Moderation Guidelines (Reproduced Snapshot)', 12 October 2021, <https://theintercept.com/document/2021/10/12/facebook-praise-support-and-representation-moderation-guidelines-reproduced-snapshot/>, accessed 7 January 2022.

be based on legitimate concerns of profitability and risk tolerance, but with the EU's fifth AMLD of 2018 bringing VASPs under the umbrella of obligated entities, that discrimination cannot be justified on such concerns alone.

At the same time, a relaxed approach is also potentially dangerous. Low to moderate risks do not mean that potential TF is not happening, with complacency leading to firms missing obvious problems – problems exacerbated by a lack of regulatory guidance on TF risks. As the senior compliance officer of a global payments services provider commented, it was easy to take the view that '[we] don't know what [TF] looks like, so [we] don't see it, so it isn't there'.[119]

Although FinTech firms confront the same challenge as legacy institutions in this regard, it is one that is perhaps more acutely felt when firms are immature, small and seeking to establish themselves. For fast-growing FinTech firms, it can be challenging to adequately invest in and implement regulatory technology (RegTech) at pace with the rate of growth, meaning firms can find themselves unprepared to deal with emerging risks.[120] FinTech firms can also face greater challenges because – as the case of the P2P lenders mentioned above highlights – they are usually smaller players within large ecosystems, with limited insight into the practices and credibility of counter-party FinTech firms with whom they need to deal.

The past regulatory approach to new financial services firms has not included providing knowledge support to specific parts of the financial sector. But the emergence of multiple FinTech firms with limited background in compliance perhaps points to the need for a change of tone, at least in the early days of growth, with more direct initial guidance on issues such as AML/CTF as firms become established. It also perhaps behoves governments to ensure that infrastructures that support good compliance – registries of commonly accepted KYC data, for one – are fully implemented to ensure that smaller firms can access the material they need to manage their risks with relative ease.

Perhaps the most welcome aspect of the FinTech response has been those firms which have sought to use more innovative methods in identifying TF risk. The use of better data and technology available to firms is positive, and should see regulatory encouragement and potential commendation. Furthermore, the evident desire of many FinTech firms to share intelligence and knowledge through FISPs is also helpful. However, it seems unlikely that private–private partnerships, lacking key inputs from law enforcement and regulators on current typologies, could be as effective as their public–private equivalents. Although FinTech membership of such state-led FISPs is not within the private sector's gift to allow, it is something that would almost certainly be of value to both sides.

119. Authors' interview with senior compliance official of major payments services provider, 27 July 2021.
120. Authors' interview with MLRO of banking services FinTech, 22 July 2021; authors' interview with head of financial crime compliance at a major payments services provider, 24 July 2021.

Evaluating social media platforms' response to the TF issue is problematic. That at least some players in the industry see it as a responsibility to take down TF-focused material as well as propaganda is a positive step, in the absence of clear legal requirements to do so. Whether motivated by reputational concerns or not, decisions to close social media accounts or take down content related to TF is a clear public good. Nonetheless, this activity still needs to be done with care, and in a way that does not destroy the potential intelligence value of the material being targeted. SOCMINT, if collected systematically, could be used to illuminate social media-enabled TF typologies and develop CTF strategies to aid disruption.[121] Another unintended consequence of the take-down approach might force a displacement effect, encouraging terrorist financiers to operate in less visible spaces and cutting off opportunities to collect intelligence produced through the use of new technologies by terrorists, streams that could be of benefit to CTF efforts.[122] Active and dedicated TF-related channels of intelligence sharing between FIUs, law enforcement agencies (LEAs) and potentially intelligence agencies would thus be essential to ensuring that key social media accounts are kept open in the interests of intelligence generation and wider-scale disruption of networks at a later date: a take-down today may be worth less than a larger disruption action tomorrow. A further challenge is that much of the relevant data or intelligence is oftentimes held by companies in foreign jurisdictions, and operating amid different regulatory restrictions on data sharing. For Europe, this is clearly an issue when it comes to potential intelligence held by social media companies based in the US. But across all platforms, de-platforming and take-downs carried out with a desire to maintain a good reputation is not a sustainable insurance policy in reducing TF risks, and indeed can be counterproductive in some areas.

121. Keatinge and Keen, 'Social Media and Terrorist Financing'; Keatinge and Keen, 'Social Media and (Counter) Terrorist Finance'.

122. *Ibid.*; Davis, 'New Technologies but Old Methods in Terrorism Financing'; Eva Entenmann and Willem van den Berg, 'Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?', International Centre for Counter-Terrorism – The Hague, 1 November 2018, <https://icct.nl/publication/terrorist-financing-and-virtual-currencies-different-sides-of-the-same-bitcoin/>, accessed 7 January 2022.

IV. Key Findings and Policy Recommendations

EIGHT KEY FINDINGS of this study have resultant policy recommendations for the EU, its institutions and agencies, and for member states themselves. By implementing these recommendations, the EU will calibrate and improve its response to the abuse of new technologies by terrorist financiers, and better utilise the unique aspects of the FinTech sector to combat TF.

Key Finding 1: The majority of the studied attacks in Europe over the last six years (74%) have been conducted by self-activating terrorists. Where information is publicly available on attack financing, new technologies rarely feature when terrorists are funding or preparing attacks, and when they do appear, they tend to be well-known, first-generation payment platforms (such as PayPal), which are ubiquitous in society in general. Most notable by their absence are VAs, where, despite concerns about their potential abuse as a way to pay for illicit items, they only appeared in one case.

- **Recommendation 1(a):** The ESAs should encourage national regulators, as well as obligated businesses in the FinTech sector, to update their risk assessments on operational TF risks, and ensure their policies, procedures and controls – especially transaction monitoring – are appropriately calibrated to this reality.
- **Recommendation 1(b):** The ESAs and Europol should review the prevalence of established payment platforms in operational TF and typologies of extremist usage, and invite these providers to collaborate on intelligence generation with a view to proactive disruption. Such collaboration should be held in a workshop series format to ensure lasting partnership.

Key Finding 2: The study has revealed more examples of new technology being used in aspects of organisational TF – for raising and transferring funds – than what can be seen in operational financing. Again, established payments services providers appear, as does social media as a means of 'pop-up' crowdfunding. In addition, there are some more notable examples of VAs being used to raise funds across the ideological spectrum. However, most subsectors of FinTech are unaffected, and there are few indications that new technologies have displaced older techniques, such as MSBs, hawala and cash couriering, which continue to dominate the scene. What appears to be more the case is the use of old and new methods together, in pragmatic combinations that suit terrorist financiers.

- **See Recommendation 1(b):** Following the pattern of Recommendation 1(b) above, European regulatory authorities should encourage national regulators and obligated businesses to update their risk assessments for organisational TF as appropriate.

- **Recommendation 2**: Europol's ECTC should conduct an analysis for publication of how different technologies and methods are being used in combination by terrorist financiers across the ideological spectrum. Such a report should provide typological detail to help obligated entities better calibrate their controls to identify suspicious activity.

Key Finding 3: Despite an improving understanding of TF risks around new technologies, this study accepts there are still significant gaps in knowledge, and further work needs to be undertaken to fill those gaps, clarify ambiguities and deepen the evidence base. There are potentially submerged organisational funding risks around VAs, and the possibility that the main subsectors of FinTech where there is a high volume of customers and transactions – online banking and payments platform providers – might feature more than is obvious at present.

- **Recommendation 3(a):** Towards elucidating this 'submerged risk', Europol should conduct a retrospective review of confidential information on past cases to clarify that certain key sectors have not featured more prominently than currently appears.
- **Recommendation 3(b):** In future, Europol should also take a more rigorous approach to systematic collection of data on TF for future TE-SATs, to identify incidence of method used in operational and organisational finance. This should be based on a centrally designed template, rather than the supply of anecdotal data by member states' law enforcement agencies.

Key Finding 4: Some of the rhetoric on the risks associated with new technologies from leading EU policymakers, and the public messaging from the Commission, appears unbalanced in light of the scale of the landscape and the levels of risk. New technology does not equal VAs alone, and novelty does not necessarily equal high risk. The rhetoric is, moreover, in contradiction to some of the EU's other stated aims. The heavy emphasis on the vulnerability of new technology sectors per se sits uneasily alongside the Commission's stated desire to promote digital and financial innovation, with a better balance needing to be struck and actively communicated.

- **Recommendation 4**: The Commission and senior officials of EU agencies should recognise publicly the scope of new technologies in the financial system and varying degrees of risk within the many subsectors. Overall, strategy towards financial innovation needs to take an integrated view of both opportunities and risk, and the Commission should develop a communications strategy that balances both.

Key Finding 5: The EU's approach of integrating most elements of FinTech into the pre-existing AML/CTF structure follows the pattern of over three decades. However, it lacks sensitivity and nuance; there are clear risks with a 'one size fits all' approach to emerging sectors that can easily be undermined by regulatory burdens. A lighter touch – such as that which has been applied to return-based crowdfunding – would have been more appropriate in subsectors at lower risk, such as insurance or investments, especially at an early stage of their development. In contrast, stronger attention and additional regulatory support should have been deployed in volume-driven subsectors such as payments or online banking.

- **Recommendation 5(a)**: At present, it will not be possible to retreat from the standardised integration of FinTech sectors into the pre-existing AMLDs. However, in the medium term, a new AML Agency, should it emerge as proposed, should review the application of AML/CTF in its new 'Single Rulebook', to ensure sensitivity to the risks and realities in each subsector. The AML Plan offers the EU the opportunity to take a more agile approach.
- **Recommendation 5(b)**: In the short term, the ESAs should produce FATF-style sector-focused guidance on applying the RBA to different FinTech subsectors. The EBA's Risk Factor Guidance (last revised in 2021) should also be updated.[123] Ideally, both should be informed by case-based examples of TF typologies developed by Europol (see Recommendation 2).

Key Finding 6: The 'digitally native' nature of many FinTech firms offers new avenues for these firms to contribute to CTF efforts outside of the STRs regime, including through the sharing and proactive analysis of some non-financial data they may hold, like a user's IP address.

- **Recommendation 6**: National FIUs should enter into dialogue with the FinTech sector in their jurisdiction to establish partnerships for data sharing as part of suspicious activity reporting. Similar considerations should be taken as the EU's AML Agency takes shape.

Key Finding 7: Social media platforms are not 'financial' tools, but the communications capabilities common to such platforms allow extremists to share financial information, or direct others how and where to send funds. This makes such platforms valuable tools for TF, a point which is yet to be recognised by the relevant EU regulation on online terrorist content. This omission needs to be addressed.

- **Recommendation 7(a):** Relevant EU regulations on terrorist content should be explicitly updated to preclude the sharing of financial information or directions for TF purposes.
- **Recommendation 7(b):** Social media platforms should also have a legal responsibility to report TF-relevant information to the national FIU, or preferably to national law enforcement or intelligence agencies with CT and/or CTF investigative responsibilities.
- **Recommendation 7(c)**: Europol should establish a secure SOCMINT portal for the submission of TF-related intelligence from social media platforms. This intelligence should be used to inform the work of the ECTC outlined in Recommendation 3.

Key Finding 8: FISPs have proved a helpful addition to the pre-existing financial intelligence sharing structures of the AML/CTF regime. At this time, the EU's FISP, the EFIPPP – a clearing house for sharing strategic intelligence and developing typologies – has limited its private sector membership to systemically significant financial

123. European Banking Authority, 'Guidelines on ML/TF Risk Factors (Revised)', <https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/revised-guidelines-on-ml-tf-risk-factors>, accessed 16 March 2022.

institutions alone. As a result, important avenues for dialogue between the long-term core stakeholders in AML/CTF and new entrants into the financial world is being lost.

- **Recommendation 8**: The EFIPPP should invite the involvement of leading European FinTechs, especially in the banking and payments subsectors, donation-based crowdfunding, VAs, and also social media, as well as relevant European trade associations. Their involvement – potentially in a new tech 'working group' – should be used to inform the work of the ESAs and Europol on better regulatory guidance and intelligence collection on TF risks.

Conclusion and Future Outlook

THIS PAPER HAS considered the extent to which new technologies have posed novel TF risks, or exacerbated those that already existed in Europe prior to the rise of FinTech. Answering that question has posed several challenges, not least of which has been definitional: the term 'new technologies' has been imprecisely used in discussions of the topic, and there has been a tendency to centre attention on the most 'exotic' of new technologies around VAs and VASPs, reducing coverage of the full terrain of FinTech or other relevant sectors.

Intimately linked with this issue of definition has been a problem of evidence. With a lack of clarity about what might be relevant to TF, public agencies and the obligated private sector firms have not been rigorous in collating evidence that would help clarify the levels of risk. As a result, the evidence in the area remains thin, informing a debate that has been shaped more by philosophical assumptions and attention-grabbing headlines than by comprehensive data. On the one hand, a 'pessimists' group, who come largely from the public sector and traditional financial services, have stressed the theoretical risks of new technologies; 'if something can be misused, it will be' might sum up their view. In the literature, the 'pessimists' argue that new technologies will: offer terrorists new channels to undertake TF; support their TF tradecraft with low transaction costs and supposed anonymity; and lead to reduced surveillance because of supposed weaker financial crime controls. On the other hand, there are the 'optimists', who largely sit within the new technology sectors, emphasising the limited amount of material demonstrating elevated TF risk; it might be said that there is a presumption here in some cases that absence of evidence is also evidence of absence.

In order to test these two hypotheses, this study has looked at the available evidence as comprehensively as possible, while also accepting the limitations imposed by the novelty of the subject matter. Overall, this study serves to narrow the divergence between the pessimists and optimists: there are TF risks from some new technologies, but it is not a generalised risk across FinTech, and is greater in some subsectors than others. TF risk is, moreover, present beyond the financial sector. Social media can exacerbate risk when used in tandem with old and new financial methods to choreograph organisational funding campaigns.

The CTF regime in the EU follows longstanding core elements, which look to obligated elements of the financial sector and other related stakeholders to act as the guardians and gatekeepers of the system. Over the last decade, EU policymakers have sought to integrate different aspects of FinTech into the pre-existing AML/CTF structures, requiring most – but not all subsectors – to meet its requirements. However, other areas, such as social media, have continued to be treated separately. This strategy, though consistent with the approach endorsed by the FATF, has a number of problems which need to be addressed.

In addressing TF risks arising from new technologies, there is a danger in assuming that these risks – or their absence – are inherent and immutable. However, the picture is likely to change over time, especially if wider societal use of different new technologies follows. Therefore, any judgements made by this study are necessarily provisional, and will need to be addressed again in years to come, driving home the importance of filling knowledge gaps and maintaining good intelligence. Although no additional recommendations arise from this point, it further underlines the importance of Europol's intelligence collection efforts and their publication in annual TE-SATs, and the need – as noted in Recommendation 3(b) – for a more systematic and thoroughgoing approach.

About the Authors

Stephen Reimer is a Research Fellow at RUSI's Centre for Financial Crime and Security Studies, where he specialises in countering the financing of terrorism and threat finance generally. His recent work has focused on self-activating terrorism finance in Europe, the national security threats posed by illicit finance, and assessing risk of terrorism financing abuse in the non-profit sector.

Matthew Redhead is a writer on financial crime and national security topics, and an independent financial crime risk consultant to the FinTech and RegTech sectors. He has previously worked in the financial services industry and the UK government.