RUSI EUROPE

Project craaft

Collaboration, Research & Analysis Against the Financing of Terrorism

Occasional Paper

A New Normal

Countering the Financing of Self-Activating Terrorism in Europe

Stephen Reimer and Matthew Redhead

A New Normal

Countering the Financing of Self-Activating Terrorism in Europe

Stephen Reimer and Matthew Redhead

RUSI Occasional Paper, May 2021

RUSI EUROPE

Project craaft

Collaboration, Research & Analysis Against the Financing of Terrorism

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.

190 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 190 years.

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

Published in 2021 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, May 2021. 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The authors would like to thank their research assistant Gabriel Mimoune, who conducted an unpublished literature review which informed Chapter II of this paper and all the individuals who volunteered to serve as expert interviewees for this research, as well as to the anonymous peer reviewers whose feedback on the draft paper was invaluable. Thanks also to Tom Keatinge, Alanna Putze and Kinga Redlowska for their support of this research project, and to Isabella Chase for facilitating a webinar discussion where some of the initial findings of this research were presented. 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

NUMEROUS DEADLY TERRORIST attacks across Europe – from the 2015 *Charlie Hebdo* attack in Paris and the Manchester Arena bombing of 2016 to the far-right firearms assault in Hanau, Germany in early 2020 – demonstrate that self-activating terrorism (sometimes referred to as lone actor or small cell terrorism) has become a major security concern for the continent.

Much of the current 'conventional wisdom' around these kinds of actors assumes that terrorist financing and a counterterrorist financing (CTF) response are not relevant to this growing threat. Reports of attacks involving little to no preparation or financial resourcing have shaped a false perception that self-activator activity produces no usable financial intelligence. This has generated a high degree of unease among both CTF professionals in law enforcement, whose role it is to use legal investigatory powers to apprehend terrorists and would-be terrorists, and practitioners in the financial services sector, whose controls and instruments are designed to identify and report abuse of the financial system by terrorists planning attacks. The natural fear is that if the private sector cannot produce the kind of financial intelligence required, then law enforcement cannot do its job as effectively as it might.

In light of this, the European Commission commissioned RUSI Europe to carry out this research study as part of Project CRAAFT,[1] which seeks to answer two related research questions:

1. How do self-activating terrorists operating in Europe conduct their financial attack preparations?
2. How should the CTF regime be changed to meet this pervasive terrorist threat?

For evidence, the research team reviewed relevant academic and policy literature and credible media reports, conducted 37 semi-structured interviews with relevant experts, reviewed 106 cases of successful and disrupted self-activated attacks in Europe between January 2015 and November 2020, and carried out three in-depth case study analyses.

Key Findings

For research question 1:

- Attack planning by self-activating terrorists can have a financial and commercial dimension that is not yet fully appreciated by practitioners.

1. See Acknowledgements for further details of Project CRAAFT.

- Self-activating terrorists' financial activity is not necessarily negligible or invisible, and they may use a range of financial channels and products, including cash, digital payments and in a small number of cases, new financial technologies, to undertake their activities.
- The economic ecosystem that self-activating terrorists (and terrorists in general) currently operate within is broad, and their financial activities also leave commercial traces, some of which may be pronounced.

For research question 2:

- CTF faces basic problems with the detection of financial intelligence because of its focus on outdated models of terrorist financing, problems which are exacerbated in small-scale but complex threats such as self-activating terrorists.
- Where the private sector provides well-prepared financial intelligence, it is often poorly aligned to investigative priorities, or poorly distributed, and therefore goes unexploited.
- Current lead-generating initiatives that could identify potential financial intelligence on self-activating terrorists have not been fully encouraged or exploited by the public sector.
- Current CTF collaborations are not structurally flexible or wide-ranging enough to tackle the self-activating terrorist problem proactively.

Recommendations

- It is vital that Europol, Eurojust and other relevant EU-level agencies work with member states' law enforcement and intelligence agencies on the collection and analysis of sensitive and publicly unavailable financial and commercial information in self-activating terrorism cases to create an evidence-based understanding of attack-planning behaviours and a library of typologies that could provide financial institutions with a better understanding of the logistics of self-activating terrorism events.

- The private sector and EU agencies have better prospects of tracing suspicious activity where cash is not used. The European Commission should therefore review the potential benefits of limiting cash payments (or requiring customer identification and verification) in the purchase of a small number of high-risk items such as ornamental or ritualistic edged weapons, or chemicals used in improvised explosive devices.

- In keeping with its wider anti-money-laundering (AML)/CTF responsibilities, the European Commission should undertake an annual review with relevant EU agencies to

ensure that its Anti-Money Laundering Directives cover all relevant emerging financial technologies and platforms that might be used by criminals and terrorists.

- The European Commission should consider developing a list of high-risk items that have been/could be used in self-activating terrorism or other attacks to guide vendor decisions on whether to execute a sale.

- The European Commission should review whether specific types of retail outlet which sell high-risk items should be encouraged to develop voluntary reporting mechanisms of suspicious items or be covered by mandatory AML/CTF monitoring and reporting requirements.

- The European Commission and relevant EU agencies should consult on ways to ensure financial institutions and other obligated entities produce better and more timely financial intelligence on self-activating terrorism. This could include:
    - The development of evidence-based self-activating terrorism typologies, case studies and supporting information (based on work in the first recommendation) to be shared with member states' governments and agencies, and the AML/CTF-obligated private sector.
    - Feasibility studies on how AML/CTF transaction monitoring platforms can best exploit modern payments data to provide a more granular view of client activity, and how new technologies could be used to get institutions closer to real-time monitoring for threat-to-life risks.

- The European Commission and relevant EU agencies should consult on ways in which CTF intelligence can be better aligned with current risk priorities and distributed to all relevant audiences. This could include:
    - The development of prioritisation and feedback mechanisms for CTF suspicious transaction reports between the public and private sectors. Responsible public agencies could set specific requirements for the kind of financial intelligence they wish to receive (such as potential self-activating terrorist activity) and provide evaluations of whether those requirements are being met.
    - The requirement that all counterterrorism-tasked intelligence services should become standard and integral elements in the distribution and feedback channels of CTF-related suspicious transaction reports.

- The European Commission and relevant EU agencies, in particular Europol and the EU's proposed new AML/CTF regulatory authority, should encourage national law enforcement agencies and regulators, and by extension the private sector, to exploit new technologies and data analytics in general, and on the self-activating terrorism problem

in particular. Ideally, this should be in collaborative environments such as financial intelligence-sharing partnerships.

- The European Commission should consider how to support such collaborations through a review and potential extension of the legal thresholds for sharing CTF data in AML/CTF and data protection law.

- The European Commission and relevant EU-level agencies should review the options for more flexible and agile CTF intelligence sharing to aid proactive self-activating terrorist identification. This could include reviewing the likely costs and operational benefits of:
    - Direct data-sharing/transaction monitoring for CTF risks by a government agency, as in France, or potentially in collaboration with the private sector.
    - The development of private–public sector intelligence 'fusion cells' to create real-time intelligence sharing on CTF issues such as potential self-activating terrorists.

It should be noted that these recommendations are based on what is practically feasible in light of current capabilities to better tackle self-activating terrorism. However, any reforms must also take into account other policy considerations, such as financial costs incurred – and who pays for them – as well as the potential effects on data privacy of increased collaboration between the public and private sectors. Although there are potential mitigants for these concerns, the decision to make the current CTF framework more responsive to the self-activating terrorism threat will require greater effort and more targeted monitoring of some individuals. The decision to take this path rests on a societal consensus that the likely costs are worth the operational benefit.

Introduction

ACCORDING TO EUROPOL, the EU's policing agency, the continent's most significant terrorist threat 'emanates from lone actors or small cells carrying out violence on their own accord without being directed by larger organisations', coming from both Islamist and far-right extremists.[1] Despite national lockdowns during the coronavirus pandemic, the threat has remained consistent and immediate. Indeed, such attacks continued throughout 2020, including a firearm assault in Vienna in November that killed four people and injured 20 others,[2] yet another instance of what has become a new normal in the security landscape of European society.

These kinds of attacks are often said to be the work of 'lone actors and small cells', with 'small cells' typically containing two or three individuals. Although the term is not inaccurate, it is sub-optimal. Instead, this research uses the term 'self-activating terrorists', a more economical descriptor which emphasises the key issue of these actors' relative operational autonomy. So far, self-activating terrorism research has focused on radicalisation and characteristics that might differentiate them from other types of terrorist actor. Key themes emerging from past research include the relevance of individuals' mental health and high levels of internet use.[3]

In contrast, studies of the logistical components of self-activating terrorism, such as terrorist financing, have lagged behind. There are understandable practical reasons for this; the growth of the self-activating terrorism threat remains relatively new, and it is arguably far easier and possibly more impactful to study the operational activities of groups or networks, such as Al-Qa'ida and the Islamic State. However, research into self-activating terrorist financial activity has also been inhibited by assumptions about its relevance. Unlike the more coordinated attacks of Islamist extremist groups common until 2015, self-activating terrorist attacks have tended to be less sophisticated and far cheaper, raising the question of whether 'terrorist financing' is a meaningful concept when it comes to self-activating terrorism.

This is an existential issue for the global CTF regime. Emerging after 9/11, the regime uses the pre-existing tools of the AML framework, such as asset freezing and suspicious activity reports, to interdict funds moving through the international financial system. As self-activating terrorists are not funded by substantial international transfers, the significance of CTF in modern counterterrorism strategies is considered largely irrelevant by some. However, these pessimistic assumptions are based on relatively limited evidence about the financial activities of self-activating terrorists.

---

1. Europol, 'European Union Terrorism Situation and Trend Report 2020', 23 June 2020, p. 19.
2. *DW*, 'Vienna Terror Attack: Police Investigating 21 Potential Accomplices', 13 November 2020.
3. Clare Ellis et al., 'Lone-Actor Terrorism', Countering Lone-Actor Terrorism Series No. 11, Final Report, RUSI, April 2016, pp. viii–ix.

The current situation is dire and untenable. The 'new normal' of self-activating terrorism requires reform across Europe to counter the financing of what Europol considers to be the main terrorist threat facing the continent. This paper is intended to fill a gap in the collective understanding of the financial behaviours of self-activating terrorists from across the ideological spectrum and to offer guidance on how CTF efforts might be shaped to the distinct contours of this threat. It seeks to answer two related research questions:

1. How do self-activating terrorists operating in Europe conduct their financial attack preparations?
2. How should the CTF regime be changed to meet this pervasive terrorist threat?

A RUSI study from 2017 laid foundations in this area by assessing the financing connected with a sample of 63 lone actor and small cell terrorist plots in the UK and France from 2000 to 2014.[4] The authors of this study noted that although there are difficulties in collating and exploiting financial intelligence on individuals' financial activities, it could still play a valuable role in public–private intelligence-sharing arrangements, especially in the wake of attacks.[5]

This paper seeks to build on the foundation set out in the 2017 RUSI study, in part by expanding the field of study to include self-activating terrorist attacks conducted across Europe. Furthermore, several examples of self-activating terrorist financial and procurement activity from the last five years (picking up from where the 2017 study ended) demonstrate that self-activating terrorism attack planning – especially more ambitious plots involving improvised explosive devices (IEDs) – can leave discernible financial traces and the imprints of commercial activity. While these financial traces will likely remain difficult to identify and share through contemporary CTF processes, this study finds that there are reasonable grounds to believe that this kind of financial intelligence – when synthesised with other types of intelligence – could make an impactful contribution both before and after an attack. This pre-attack contribution may come about if a more agile means of delivering intelligence from the private to the public sector could be designed, marking a departure from the findings of this study's predecessor, which focused on the importance of post-attack intelligence sharing.

The paper explores these issues in four chapters. Chapter I outlines the scope and methodological basis of the study. Chapter II details the evolving understanding of self-activating terrorist financing and procurement behaviours. Chapter III explores how the CTF regime has addressed the emerging self-activating terrorism threat to date. The paper concludes by outlining ways in which financial intelligence on self-activating terrorists might be more effectively gathered and shared in the future.

4. Tom Keatinge and Florence Keen, 'Lone-Actor and Small Cell Terrorist Attacks: A New Front in Counter-Terrorist Finance?', *RUSI Occasional Papers* (January 2017). This study excluded plots in Northern Ireland.
5. *Ibid*.

I. Methodology

IN RESEARCH WORK on any aspect of terrorism, clear definitions are a fundamental foundation, given the complexity of debate around the subject. Equally important is providing a transparent understanding of the scope and manner of collection of data, especially as so much data around the topic is highly sensitive and held by official agencies. The following section provides a brief outline of the paper's approach to these issues.

Definitions

A fundamental challenge for this paper has been defining 'lone actor' and 'small cell' terrorism,[6] and the resulting search for a comprehensive term to encompass both. The designation 'lone actor' is particularly ambiguous; even if terrorist attacks are undertaken solo, perpetrators are rarely completely isolated from wider extremist or radical milieus.[7] A Swedish official interviewed for this study remarked that lone actors and small cells were 'not part of a group, not part of a network, but not part of a vacuum, either'.[8] Defining this threat by the number of people involved – usually three or fewer – is similarly dissatisfying, leaving open the possibility of 'small cells' that are under the close direction or operational control of a network or group, or 'large cells' of four or more that are not.

As a consequence, this paper will instead be using the term 'self-activating terrorists', developed by Matthew Feldman.[9] Self-activating terrorists refers to those who are broadly in control of the initiation, planning and execution of their attacks. This encompasses actors that have links to wider extremist networks, while also recognising that they exhibit some degree of operational

6. This study follows the UN's 1994 General Assembly Declaration on Measures to Eliminate International Terrorism, defining terrorist acts as 'criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes'. See UN, 'Declaration on Measures to Eliminate International Terrorism', December 1994, <https://legal.un.org/avl/ha/dot/dot.html>, accessed 20 December 2020.
7. Paul Gill, *Lone Actor Terrorists: A Behavioural Analysis* (Abingdon: Routledge, 2015), pp. 11–15; Bart Schuurman et al., 'Lone Actor Terrorist Attack Planning and Preparation: A Data-Driven Analysis', *Journal of Forensic Sciences* (Vol. 63, No. 4, 2018), pp. 1191–200; Bart Schuurman et al., 'End of the Lone Wolf: The Typology That Should Not Have Been', *Studies in Conflict & Terrorism* (Vol. 42, No. 8, 2019), pp. 771–78.
8. Author videoconference interview with the Swedish Security Service, 2 July 2020.
9. For a discussion of the limitations of the 'lone wolf' concept that precipitates this understanding of self-activating terrorists, see Gerry Gable and Paul Jackson, 'Lone Wolves: Myth or Reality', *Searchlight*, 2011, <nectar.northampton.ac.uk/6014/1/Gable20116014.pdf>, accessed 22 January 2020; Matthew Feldman, 'Comparative Lone Wolf Terrorism: Toward a Heuristic Definition', *Democracy and Security* (Vol. 9, No. 3, 2013).

autonomy. Of course, the self-activating terrorism definition is far from 'water-tight'. There will always be 'boundary' cases, where determining the level of actors' personal sovereignty is difficult. This paper has taken a broad approach, including attacks prepared and mounted without close direction or support, but also those potentially inspired and encouraged from outside the immediate attack cell.

Scope

The paper investigates the financial contours of recent self-activating terrorist attack planning in Europe, and the effectiveness of current EU CTF measures to detect and disrupt such preparations. Sponsored by the European Commission with a view to developing potential CTF reforms, it looks at cases from across the political spectrum, including religiously-inspired ideologies such as Islamist extremism, and both successful and disrupted attacks. It also focuses on attack planning in the EU and neighbouring states (the UK, Norway and Switzerland). To ensure that this paper is relevant to current self-activating terrorist modus operandi, it looks at material from 106 cases that took place between 1 January 2015 and 30 November 2020. Although this date range is somewhat arbitrary, this period does cover the time from when Europol recognised the particular significance of lone actors and small cells.[10]

Data Collection and Analysis

The project ran from January to December 2020, with the research process comprising a narrative review of available English-language academic and policy literature published to the end of June 2020.

Semi-structured interviews were conducted to assess the current state of knowledge on self-activating terrorist financial activities and CTF effectiveness. Interviewees were selected from four categories of stakeholder with relevant interest and involvement in terrorism and CTF: researchers; public officials; law enforcement officers; and private sector AML/CTF compliance specialists.

Representatives from each of these different categories were identified in four 'target' countries: France; Germany; the UK; and Sweden. France, Germany and the UK were chosen because they were subject to the largest number of relevant attacks in the period of study, while Sweden was included because of its significant terrorism research community. Initial expectations were that two interviews per category in each country would be completed, totalling 32 interviews.

Due to challenges posed by the coronavirus pandemic, it was not possible to arrange interviews in every stakeholder category in all four countries, and in four instances, interviewees requested the opportunity to respond in writing because of work pressure. Where stakeholders with

10. Europol, *European Union Terrorism Situation and Trend Report (TE-SAT) 2016* (The Hague: European Police Office, 2016), p. 5.

relevant expertise were available in other European jurisdictions, further interviews were conducted. In total, 33 verbal interviews and four 'paper' interviews were completed.

The literature review and interviews were also supplemented with a review of available English-language reporting from mainstream national print and broadcast media from all in-scope countries over the period. This review identified 106 self-activating terrorism cases from 14 jurisdictions,[11] although this is unlikely to be exhaustive. Many disrupted cases go unreported, and where self-activating terrorists have been killed during an attack, trials do not always occur or are subject to legal restrictions on public reporting.

11. Austria, Belgium, Croatia, Denmark, Finland, France, Germany, Italy, Latvia, Netherlands, Norway, Poland, Sweden, and the UK.

II. Funding and Resourcing

THE SELF-ACTIVATING TERRORISM threat has now been on the rise in Europe for over a decade. For example, Petter Nesser found that between 2008 and 2014, Europe witnessed a 40% rise in self-activating terrorist attacks, and annual operational updates from Europol have suggested that this trend is continuing.[12]

But, as Eric Price noted in his survey of terrorist financing literature between 2001 and 2013, academic research during that period focused largely on the financial activities of organised groups and networks,[13] with a body of literature only just beginning to emerge on the financial behaviours and funding strategies of self-activators.[14]

According to the current consensus, self-activating terrorists – regardless of ideology – are likely to use their own earned income or borrowed money to fund or resource their attacks, or resort to petty criminality if they are unable to meet expenses using legitimately sourced funds.[15] The literature suggests that because of the limited capabilities of most self-activating terrorists, attacks tend to be relatively modest and therefore simpler to fund and resource.

Evidence from the last five years in Europe tends to support these assessments. However, there are several significant examples where attack ambitions have been more sophisticated, requiring extensive preparation. Although this suggests that financial intelligence around the preparation for a self-activating terrorist attack is likely to be limited in many cases, there will also be many where it is not. Indeed, the more ambitious the plans of the self-activating terrorist, the more intelligence that is likely to emerge. It is also worth recalling that many actual and potential

12. See, for example, Europol, *European Union Terrorism Situation and Trend Report 2019* (The Hague: Europol, 2019).
13. For an overview of the literature on terrorist financing between 2001 and 2013, see Eric Price, 'Literature on the Financing of Terrorism', *Perspectives on* Terrorism (Vol. 7, No. 4, 2013), pp. 112–30; Financial Action Task Force (FATF), 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', updated October 2020; UN Security Council Resolution 1373, 28 September 2001, S/RES/1373.
14. See, for example, Emilie Oftedal, *The Financing of Jihadi Terrorist Cells in Europe* (Kjeller: Norwegian Defence Research Establishment, 2015); Michael Freeman, 'The Sources of Terrorist Financing: Theory and Typology', *Studies in Conflict & Terrorism* (Vol. 34, No. 6, 2011), pp. 461–75; Rajan Basra and Peter Neumann, 'Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus', *Perspectives on Terrorism* (Vol. 10, No. 6, 2016), pp. 25–40; Petter Nesser, Anne Stenersen and Emilie Oftedal, 'Jihadi Terrorism in Europe: The IS-Effect', *Perspectives on Terrorism* (Vol. 10, No. 6, 2016); Schuurman et al., 'Lone Actor Terrorist Attack Planning and Preparation'.
15. Freeman, 'The Sources of Terrorist Financing'.

self-activating terrorist plots that have been disrupted have evidenced the ambitions and capabilities to undertake more than just small-scale attacks.

Terrorist Finance

In the wake of 9/11, there was a strong presumption that prominent terrorist networks such as Al-Qa'ida were transferring funds through the financial system to support the activities of their operatives around the world – a top-down approach, where funds were accompanied by direction and came from the centre of the network. As government surveillance and international cooperation have proven increasingly effective in degrading organised groups' capabilities and command structures, elements within the movement have switched from directing attacks towards stimulating autonomous activity via social media and the online world.[16] Models of financing followed a similar trajectory. As Emilie Oftedal details, based on a study covering 1994 to 2013, plots reliant on international funding began to wane in the immediate aftermath of 9/11.[17]

Oftedal also suggests that this pattern has largely carried over into the behaviours of self-activating terrorists, as core groups and networks have declined, with funding coming mostly from banal and legitimate sources, including wages, savings, loans and state benefits.[18] Attacks have remained cheap and relatively easy to fund – 80% of the Islamist extremist self-activating terrorist attacks in Europe in Oftedal's study cost less than $10,000, suggesting that attack preparations do not leave a large financial footprint.[19]

Although research into far-right extremist financing is more limited, early indications tend to suggest that they too have largely derived funds from relatively unremarkable sources.[20] According to Bart Schuurman and colleagues, whose sample covered single-issue, far-right and Islamist self-activating terrorists, only 13% had attempted to secure external financial support for their attack.[21] For example, Anders Breivik, who launched truck bomb and firearms assaults in

16. Petter Nesser, *Islamist Terrorism in Europe* (London: Hurst, 2018), p. 267; Author videoconference interview with former UK intelligence officer, 20 May 2020.
17. Oftedal, *The Financing of Jihadi Terrorist Cells in Europe,* p. 15.
18. *Ibid*.
19. *Ibid*., p. 24. In this study, Oftedal surveyed the financing of 40 terrorist cells that plotted attacks in Europe between 1994 and 2013.
20. See 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; Bethan Johnson, 'Financing Right-Wing Extremism and Terrorism', Project CRAAFT Research Briefing (No. 5).
21. Schuurman et al., 'Lone Actor Terrorist Attack Planning and Preparation', p. 1196. Schuurman and colleagues sampled the attack planning and preparation of 55 lone actors in Europe and North America from 1986 to 2015.

Oslo and Utøya, Norway, in July 2011,[22] used personal savings from selling fake online diplomas and other investments to prepare for his attack.[23]

Sources of Funding

This paper's review of cases between 2015 and 2020 has confirmed the results found in Oftedal, Nesser and colleagues and others, with regard to the importance of legitimate, albeit misused, sources of self-activating terrorists' attack funding, where some of that misuse involves fraud – in particular, income, loans and state benefits, but also through the sale of personal items and the solicitation of funding from associates.[24] Although limitations on publicly available data prohibit a quantitative analysis of the relative incidence of each type of funding stream, case studies highlight the different funding streams that self-activating terrorists use:

- **Income**: Mohamed M, who planted an IED in Lyon in May 2019, is believed to have bought components with the funds he generated teaching IT online through a private tutoring platform.[25] In another example, Mohammed Rehman and his wife Sana Ahmed Khan were convicted in 2015 of planning a terrorist attack in London involving 11kg of fertiliser for an IED, which was purchased using Khan's wages (in addition to payday loans).[26]
- **Credit and Loans**: Amedy Coulibaly, who launched a series of firearms attacks in Ile de France in early 2015, funded his activities in part through a €6,000 consumer loan he secured using fraudulent documentation in 2014.[27] In another case, Salman Abedi, the Manchester Arena bomber, appears to have used some of his student loan to support his operational activities.[28]
- **State Benefits**: Salman and Hashem Abedi's other major source of income was the state benefits paid into their mother's UK bank account, to which they had access while their mother was in Libya. The account received housing benefit, tax credits and child benefit

22. Schuurman et al., 'End of the Lone Wolf'; author videoconference interview with Florence Keen, 1 May 2020.
23. Torgeir Husby and Synne Sørheim, 'Rettspsykiatrisk erklæring 1' ['Forensic Psychiatric Statement 1'], 11 August 2011, p. 77, <https://www.vg.no/spesial/2011/22-juli/psykiatrisk_vurdering/>, accessed 20 April 2020.
24. Oftedal, *The Financing of Jihadi Terrorist Cells in Europe*, p. 7.
25. Authors' videoconference interview with French law enforcement official, 9 July 2020.
26. *Berkshire Live*, 'Reading Terror Plotters Husband and Wife May Never be Released', 30 December 2015, <https://www.getreading.co.uk/news/reading-berkshire-news/reading-terror-plotters-husband-wife-10667833>, accessed 4 January 2020.
27. Basra and Neumann, 'Criminal Pasts, Terrorist Futures', p. 35.
28. *BBC News*, 'Manchester Arena Bomb Parts "Bought By Brothers Using Mum's Card"', 10 February 2020; John Scheerhout, 'All the Evidence in the Manchester Arena Trial, Day by Day', *Manchester Evening News*, 20 August 2020, <https://www.manchestereveningnews.co.uk/news/hashem-abedi-evidence-manchester-arena-18790131>, accessed 2 November 2020.

worth over £500 a week during two periods within the seven years that the family lived between the UK and Libya.[29]

- **Personal Donations**: In a small number of cases, aspiring self-activating terrorists have also sought donations from ideologically sympathetic associates to support their preparations. In a video released after his attack, for example, Coulibaly declared that he had donated several thousand euros to Saïd and Chérif Kouachi so that they could finish preparing for their own firearms attack on the offices of *Charlie Hebdo*.[30] Adel Kermiche, one of the two knife attackers at a Normandy church in July 2016, is also believed to have asked friends for money before his attack.[31]
- **Sale of Personal Effects**: Mohamed Lahouaiej-Bouhlel, who carried out a vehicle attack in Nice in July 2016, bought a firearm for €1,400 and rented the lorry he used for the attack using cash from the €3,000 sale of his own car.[32]

Alongside the misuse of legitimate finances, there has been a consistent stream of illicit funds being used to support the operational activities of many Islamist extremists, especially in France. Many of these self-activating terrorists have also come from what Peter Neumann has described as 'Generation ISIS' – a group of younger extremists who have been shaped primarily by mobile technologies and social media and exhibit a common habit of flitting between a jihadi and petty criminal lifestyle.[33] For example, the Kouachi brothers were able to buy weapons in part with the proceeds of drug trafficking and illicit trade in counterfeit products,[34] while Ayoub El-Khazzani, who attempted to perpetrate a firearm attack on a train between Brussels and Paris in August 2015, had previous criminal convictions and was at least partly funded through criminal activities such as robbery and the sale of drugs.[35]

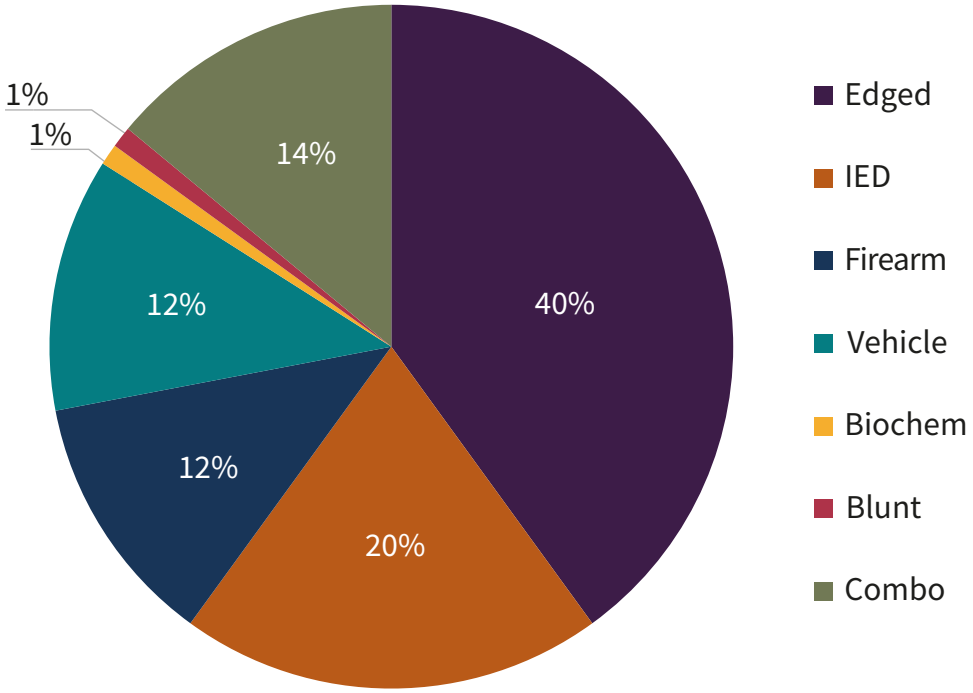
---

29. *Ibid*.
30. *L'Express*, 'Amedy Coulibaly a pu financer ses attentats par un crédit à la consommation', 1 April 2015, <https://www.lexpress.fr/actualite/societe/amedy-coulibaly-a-pu-financer-ses-attentats-par-un-credit-a-la-consommation_1640488.html>, accessed 20 April 2020.
31. Ben Farmer et al., 'France Church Attack: Second Normandy Priest Killer Named', *The Telegraph*, 27 July 2016.
32. Authors' videoconference interview with French law enforcement official, 9 July 2020.
33. Authors' videoconference interview with Peter Neumann, 4 May 2020; authors' videoconference interview with former senior UK law enforcement officer, 4 June 2020; authors' videoconference interview with Swedish financial intelligence unit (FIU) official, 3 July 2020; authors' videoconference interview with Nicholas Ryder, 24 April 2020.
34. Union des Fabricants (UNIFAB), 'Contra-Façon et Terrorisme: Rapport 2016', p. 16, <https://www.inpi.fr/sites/default/files/rapport-a-terrorisme-2015_fr.pdf>, accessed 21 April 2021; Oftedal, *The Financing of Jihadi Terrorist Cells in Europe*, p. 63.
35. Peter Neumann, 'Don't Follow the Money: The Problem with the War on Terrorist Financing', *Foreign Affairs*, July/August 2017, p. 98; Louise Shelley, '"ISIS" Members Depend on Petty Crime to Function in Europe', *New York Times,* 20 November 2015; Angelique Chrisafis, 'Life of Paris Attacker Omar Ismail Mostefai: From Petty Crime to Radicalisation', *The Guardian*, 16 November 2015.

Attacks, Logistics and Channels of Procurement

The choice of weapon is one of the most crucial decisions related to financing that a self-activating terrorist must make, and most use one of four types (see Figure 1), or a combination of these – edged weapons such as knives or machetes, IEDs, vehicles or firearms.[36] Attacks with edged weapons are used as the main weapon in 40% of cases, with 20% of attacks using IEDs, 12% using vehicles and 12% using firearms. Recent self-activating terrorist attacks by far-right extremists show a particular attraction to firearms, as seen in Halle and Hanau in Germany, in October 2019 and February 2020, respectively (see below).[37]

Figure 1: Main Weapons Types Used in Self-Activating Terrorist Attacks in European States in Scope, January 2015–November 2020



Source: Authors' research, see Annex for further details.

36. Edwin Bakker and Beatrice de Graaf, 'Lone Wolves: How to Prevent This Phenomenon?', International Centre for Counter-Terrorism – The Hague, Expert Meeting Paper, November 2010.
37. Oliver Moody, 'Germany Synagogue Attacker Used Gun Manual from UK Enthusiast Philip Luty', *The Times*, 11 October 2019; Justin Huggler, 'Tobias Rathjen: Hanau's Disturbed Far-Right Gunman Not on Any German Police Watchlists', *The Telegraph*, 20 February 2020.

Just as the funding, resourcing and logistical requirements around each style of attack differ (creating different imprints in financial or commercial activity), the pattern in the cases of the last five years suggests that there is also a variety of ways in which attackers use their funds to resource and prepare for an attack.

Some attack preparations occur over a prolonged period, as evidenced by self-activating terrorists who exhibit a tendency to stockpile a wide variety of dangerous items, not all of which can be used in one attack. Chérif Chekatt, the Strasbourg Christmas market bomber of December 2018, was found to have a large cache of guns and grenades at his home – more than could be used for one attack – and Mohamed M is also reported to have collected materials that could have been used for multiple, and in fact more powerful, IEDs than the one he planted.[38] In some cases, individuals who are not planning an imminent attack can accumulate weapons. In December 2018, Fatah Mohammed Abdullah was arrested in Newcastle for encouraging two individuals in Germany to undertake an attack. When police searched his property, however, they found that he too had a store of weapons that might be used in an attack, including fireworks, a detonator, a pocket knife, a balaclava and 200g of sulphur powder.[39]

However, more often, attack preparations, mostly centred on weapons procurement, are carried out in the short term. Although there is no set pattern for how this occurs, different types of attack tend to exhibit common themes around their preparation.

Edged Weapons

One of the common assumptions about edged weapons is that attackers simply use knives they already have at home. However, it is not always clear that they do. For example, Safia S, who attacked a police officer with a knife in Hanover in February 2016, used a standard kitchen knife that German officials interviewed for this project believed *could* easily have come from her own home, but may have been bought specifically.[40] Moreover, in other instances some attackers purchase edged weapons specifically for an attack. For example, the knives used in Khalid Masood's attack in Westminster in March 2017, and the three-man attack on the areas around London Bridge in June 2017, were purchased from major supermarkets.[41]

Far-right attackers have purchased symbolic weapons via specialist retailers. Anton Lundin Pettersson, for example, who attacked a school in Trollhättan, Norway, in October 2015,

38. Authors' videoconference interview with French law enforcement official, 9 July 2020.
39. Crown Prosecution Service, 'Daesh Fanatic Jailed for Masterminding 8,000 Matches Terror Attack', 26 June 2020, <https://www.cps.gov.uk/cps/news/daesh-fanatic-jailed-masterminding-8000-matches-terror-attack>, accessed 5 January 2020.
40. Authors' written correspondence with German officials, 8 October 2020.
41. Max Hill, *The Westminster Bridge Terrorist Attack* (London: The Stationery Office, 2018), p. 43; *BBC News*, 'London Bridge Inquest: Attacker "Bought Pink Knives from Lidl"', 29 May 2019.

specifically purchased a replica Viking sword and a Japanese ritual knife, along with items of Nazi memorabilia, to use in his attack.[42]

Vehicles

It would also seem reasonable to assume that vehicles would be easy to procure because of high levels of car ownership in Europe. However, the vehicles used in attacks over the last five years have tended to be larger commercial vehicles, such as vans and trucks, probably because of their potential to cause more casualties. Ownership of these kinds of vehicles is less widespread, and in a number of cases – the Nice promenade attack of July 2016, the Finsbury Mosque attack of June 2017 and the London Bridge attack, also in June 2017 – the attackers sourced the vehicles by renting them from commercial providers. Where this proved infeasible, either because of lack of funds or relevant paperwork to support rental due diligence, attackers have in some instances simply stolen the vehicles instead, as occurred in Stockholm in April 2017, when Rakhmat Akilov drove a stolen truck into a department store.[43] As with attacks using edged weapons, the need for finance and preparation is limited when it comes to attacks using vehicles.

IEDs

Although still relatively 'cheap', this kind of attack clearly requires greater time and procurement activity to execute. A surprising number of those looking to build chemical-based IEDs have been able to buy what they require openly, usually online, given that many of the individual components for a device are relatively mundane. The Abedi brothers purchased many of the ingredients for the Manchester Arena bomb via Amazon,[44] as did Ahmad Hassan, who planted an IED on an underground train in Parsons Green, London, in September 2017. Notably, Hassan used an Amazon voucher he had won at school towards his purchase of hydrogen peroxide.[45] Other general online outlets also feature in several cases, such as eBay, and would-be self-activating terrorists have also sought out specialist online suppliers. Anwar Driouich, a far-right extremist from Middlesbrough, was arrested in August 2019 after making an online order for 10kg of ammonium nitrate from a company called Aqua Plants Care.[46]

Although online purchases have played a significant role, self-activating terrorists have also used physical stores, especially to source the non-explosive elements of the potential device. Aydin Sevigin, arrested in Stockholm in February 2016, sought to build an IED using a pressure

42. Asa Erlandsson and Reid Meloy, 'The Swedish School Attack in Trollhättan', *Journal of Forensic Sciences* (Vol. 63, No. 6, 2018).
43. David Keyton, 'Uzbek Stockholm Truck Attacker Had Pledged Allegiance to IS', *Associated Press*, 13 February 2018.
44. Scheerhout, 'All the Evidence in the Manchester Arena Trial, Day by Day'.
45. Bethany Minelle, 'Parsons Green Accused Ahmed Hassan "Used School Prize to Buy Bomb Materials"', *Sky News,* 7 March 2018.
46. *BBC News*, 'Middlesbrough Fantasist Anwar Driouich Jailed for Explosive Substance'.

cooker he had bought from the home-furnishing store IKEA, and the Abedi brothers are reported to have made several trips to hardware and DIY stores over the four months in which they prepared the Manchester Arena attack.[47]

One final aspect of the preparation of IEDs is the need for a secure space in which to store components and prepare the device. In several instances – the Lyon attack, the Parsons Green attack, and the preparations of Mohammed Rehman – the self-activating terrorists have used their own residences, whether as lodgers, renters or owners, in which to receive and collate their materials.[48] However, preparations can be complex enough to require further accommodation, and the Abedi brothers secured further properties – two of which were rented – to undertake preparations, both of which were found using the peer-to-peer online classifieds marketplace, Gumtree. The brothers also used Gumtree to buy a car in which to store IED components while they visited Libya in April 2017. When purchasing the car, they told the vendor they were going to use the vehicle for Uber deliveries.[49]

Firearms

Arguably the most difficult weapons to procure are firearms, largely due to strong national legislation on gun ownership in many European countries, underpinned by the European Firearms Directive introduced initially in 1991. This has meant that, in cases where operatives have sought to attain firearms, it has often proved difficult to do so without some kind of pre-existing legal access. Tobias Rathjen, the attacker who targeted two shisha bars in the German city of Hanau in February 2020, was a registered marksman who already legally owned guns which he had purchased online.[50] In another case, Stephan Balliet, who attacked a synagogue in Halle, Germany, in October 2019, was already proficient with firearms from military training, and is reported to have made the weapons he used himself.[51]

Due to such firearms controls, many self-activating terrorists have resorted to criminal connections to acquire firearms. For those with pre-existing criminal associates, such as Omar Abdel Hamid El-Hussein, attacker of the Krudttønden Café and Copenhagen synagogue in February 2015, this proved relatively easy.[52] For those without connections, success was

47. Scheerhout, 'All the Evidence in the Manchester Arena Trial, Day by Day'.
48. Authors' videoconference interview with French officials, July 2020.
49. *Ibid*.
50. Huggler, 'Tobias Rathjen'.
51. Moody, 'Germany Synagogue Attacker Used Gun Manual from UK Enthusiast Philip Luty'.
52. Oftedal, *The Financing of Jihadi Terrorist Cells in Europe*, p. 37. French police also link his procurement to the general increase in guns in violent crime in France at roughly the same time. See Andrew Osborn, 'French Gunman's Arsenal Spotlights Illegal Arms Trade', *Reuters*, 23 March 2012. Police estimated the price of Omar Abdel Hamid El-Hussein guns at roughly €10,000. Also see Nils Duquet and Kevin Goris, *Firearms Acquisition by Terrorists in Europe* (Brussels: Flemish Peace Institute, 2018), p. 137.

limited. Ali David Sonboly, the far-right Munich shooter of July 2016, obtained firearms illegally despite having no prior criminal links,[53] but this appears to be a rare exception.

Financial Operating Methods

Cash Versus Digital

While some self-activating terrorists, such as the Hanover attacker Safia S,[54] lack any personal financial infrastructure, many other attackers with more settled lives do appear to have had conventional financial products. The Abedi brothers managed their mother's HSBC account in her absence, and Salman Abedi also had accounts with at least two different UK high street banks.[55] But even where high street retail accounts are not present, some attackers have used non-banking financial services. Mohamed M, for example, used his Payoneer accounts to receive payments from Udemy.[56] Chekatt also had PayPal, and a Nickel payment account, which can be opened at a tobacconist or newsagent.[57]

Previous research has tended to suggest that self-activating terrorists have operated primarily in cash for operational procurement, to avoid creating a digital trail of transactions. For example, in the run up to the Nice attack, Lahouaiej-Bouhlel made significant cash withdrawals from his retail bank account over a two-week period, and these funds subsequently went towards the cash purchase of a vehicle and a weapon for the attack.[58] There is a similar pattern among far-right attackers. Pettersson, for example, took the last of his money from the bank during a two-week preparatory phase prior to his attack. What was not spent in this period was left on his brother's kitchen table before he executed his plot.[59]

Nonetheless, the cases of the last five years do not suggest that those planning for more ambitious attacks have been able to procure items without at least some potentially traceable transactions. For example, Mohamed M purchased components for his IED on Amazon using a credit card,[60] and Salman Abedi is reported to have made several of the payments for his last shopping trips prior to his attack using his own retail debit card. [61]

53. Duquet and Goris, *Firearms Acquisition by Terrorists in Europe*, p. 60.
54. Authors' written correspondence with German officials, 8 October 2020.
55. *BBC News*, 'Manchester Arena Bomb Parts "Bought by Brothers Using Mum's Card"'.
56. Payoneer is a financial services platform that specialises in facilitating payments to individuals who sell goods or services via online marketplaces such as eBay, AirBnb or Udemy.
57. Authors' videoconference interview with French law enforcement official, 9 July 2020.
58. *Ibid*.
59. Erlandsson and Meloy, 'The Swedish School Attack in Trollhättan'.
60. Authors' videoconference interview with French law enforcement official, 9 July 2020.
61. Tom Parmenter, 'Salman and Hashem Abedi: The Brothers Who Bombed Manchester', *Sky News*, 19 August 2020; Scheerhout, 'All the Evidence in the Manchester Arena Trial, Day by Day'.

Virtual Assets

In the last five years, there have been a number of cases of self-activating terrorists demonstrating proficiency in virtual assets. Mohamed M purchased cryptocurrencies via crypto exchanges such as Coinmama.[62] There have also been some examples of would-be self-activating terrorists using them for operational planning purposes. Steven Bishop, for example, who was arrested in October 2018 while planning a mosque bombing in London, is reported to have used virtual assets on the dark web to purchase a detonator for his proposed device.[63] However, such individuals appear to remain in a minority at present – a view borne out in interviews with private and public sector professionals in France, Germany, Sweden and the UK for this study. Although virtual assets appear in some cases as a way of paying for illicit items for terrorist purposes, they do not, so far, appear to form a trend.[64]

Other Preparation Behaviours

Countermeasures

A number of self-activating terrorists appear to have taken intentional countermeasures to avoid detection during procurement. The Manchester Arena bombers took a range of diversionary financial techniques and were careful to distribute risk by asking a number of family and friends to buy parts for the IED online – which they claimed to be for a car or a generator in Libya – saying that they had lost bank cards or were short of money.[65] The brothers also used their mother's debit card and bought items under an alias online. On 20 March 2017, they set up an email address, 'bedab7jeana@gmail.com' (meaning 'to slaughter we have come' in Arabic), with which they then created a new Amazon account and purchased 30 litres of hydrogen peroxide under the customer name 'John O'Brian'.[66] Other countermeasures have included attempts to disguise the significance of items by making additional purchases to enhance the seeming banality of the purchase. Khalid Ali, for example, who was arrested in central London prior to launching a knife attack in April 2017, bought a potato masher and other kitchen utensils along with the three knives he intended to use to kill police officers at Westminster.[67]

---

62. See Coinmama, 'About', <https://www.coinmama.com/about-us>, accessed 13 October 2020.
63. John Simpson, 'Racist Alcoholic Plotted to Become UK's First Far-Right Suicide Bomber', *The Times*, 9 April 2019.
64. Authors' videoconference interview with Swedish Security Service, 2 July 2020; authors' videoconference interview with HSBC bank, 26 April 2020; authors' videoconference interview with Lloyd's bank, 27 April 2020.
65. Daniel De Simone, 'The Road to the Manchester Arena Bombing', *BBC News*, 17 March 2020.
66. *Ibid*.
67. *Chester Standard*, 'Al Qaida Bomb-Maker Faces Jail Over Plot to Murder MPs in Whitehall', 26 June 2018, <https://www.chesterstandard.co.uk/news/national-news/16314954.al-qaida-bomb-maker-faces-jail-plot-murder-mps-whitehall/>, accessed 25 February 2021.

Burst Activity

A final aspect of the financial behaviours around attack planning has been described as 'burst activity', which is not necessarily related to the attack, but is suggestive of a changing pattern of behaviour. Magnus Normark and Magnus Ranstorp have argued that unusual financial behaviours are common among self-activating terrorists immediately before attacks,[68] and there are instances of unusual activity taking place in cases from this paper's sample. For example, attackers may withdraw large amounts of cash, such as the withdrawals made by the Abedi brothers[69] or Lahouaiej-Bouhiel, who made four cash withdrawals of around €2,000 during his own preparations.[70] A few days before the attack, he was €200 overdrawn on his account, and faced several denials of service from ATMs.

Another example of burst activity is a disproportionately high number of credit requests or attempts to take out large loans. Coulibaly also made several loan requests in a short period, failing with most but succeeding with one on the basis of fraudulent documentation. He also took the unusual step of withdrawing his retraction rights on the loan when he had secured it, so he could receive the money in eight rather than 14 days.[71]

One further behaviour is the transfer of large funds overseas shortly before an attack, possibly to ensure that an attacker's unused funds are placed in the hands of extremist associates rather than allowing them to be frozen by the authorities after their attack. In March 2017, Salman Abedi asked a friend to help him to transfer £1,200 to a company in China.[72] Abdullah Al-Hamahmy, who launched a machete attack on police at the Louvre in Paris in February 2017, is reported to have made two money transfers of €3,000 and €2,000 to a fellow Egyptian based in Poland shortly before the attack.[73]

Assessment

The review above confirms some of the conventional wisdom on the financial, procurement and commercial aspects of attack planning by self-activating terrorists. Broadly speaking, self-activating terrorists who lack funds will perpetrate attacks with correspondingly simple weapons and low magnitudes of lethality, most commonly using edged weapons. However, this does not mean that self-activating terrorist attacks are inherently necessarily less fatal or impactful than those organised by groups. As demonstrated by the cases in this study, some self-activating

68. Magnus Normark and Magnus Ranstorp, *Understanding Terrorist Finance: Modus Operandi and National CTF-Regimes* (Stockholm: Swedish Defence University, 2015), pp. 23–24.
69. *Ibid*.
70. Authors' videoconference interview with French law enforcement officials, 9 July 2020.
71. *Le Point*, 'Amedy Coulibaly avait contracté un crédit de 6 000 euros', 14 January 2015, <https://www.lepoint.fr/societe/amedy-coulibaly-avait-contracte-un-credit-de-6-000-euros-14-01-2015-1896379_23.php>, accessed 20 August 2020.
72. Scheerhout, 'All the Evidence in the Manchester Arena Trial, Day by Day'.
73. *Irish Times*, 'Louvre Attack Suspect Says Islamic State Had Not Given Him Orders', 8 February 2017.

terrorist attacks can have devastating effects if well executed, even when relatively simple and 'cheap'. For example, in this study's French sample of 35 attacks, only in two instances – the *Charlie Hebdo* shootings of January 2015 and the Nice truck ramming of July 2016 – did the attacks result in deaths in double figures. Although the two *Hebdo* attackers were theoretically more 'lethal' than Lahouaiej-Bouhlel, using firearms rather than a truck, Lahouaiej-Bouhlel killed many more people – 86, rather than 17. Despite the truck being an 'everyday' and relatively easy to access item, it still inflicted greater damage than guns.

The lethality of attacks conducted by self-activating terrorists is not just a function of operational autonomy and limited finances, but other factors such as levels of expertise, confidence, ambition and the permissiveness of their operating environment. The Manchester Arena case demonstrates that, with an unfortunate combination of circumstances, 'cheap' and 'simple' self-activating terrorist attacks can be extremely dangerous, and many of them could also have been much worse if other contextual factors had been different. In the Hanover case, Safia S carried out her attack with a knife only because she could not source a firearm. Without a bank account or other access to funds, but just as importantly without the connections to organised crime or other such contacts to even find a firearm to buy, her attack was destined to be of relatively low impact with only one person injured.

Compare this to the Lyon case, where Mohamed M's financial resources gave him a broader scope to commit a more lethal attack. Even so, his funds were not commensurate with the magnitude of the attack he perpetrated, suggesting the presence of another inhibiting factor – possibly a lack of expertise in constructing an IED. Indeed, access to lethal weapons does not always indicate a capacity to use them effectively. For example, when Norwegian Philip Manshaus attacked an Islamic centre in Oslo in 2019, he was unable to injure or kill any worshippers with a rifle and a shotgun and was apprehended by a 65 year old.[74]

A further common assumption about self-activating terrorists and terrorist financing is that cheap attacks are also financially and commercially 'invisible'. This can be the case, especially with the use of edged weapons. However, what a review of the sample suggests is that self-activating terrorist financial activity is more complicated than is commonly assumed. Self-activating terrorists can and do draw attention to themselves through their financial and procurement activity, and the more sophisticated and ambitious their plans, the more attention they draw.

74. *BBC News*, 'Norway Mosque Attack: Bruised Suspect Manshaus Appears in Court', 12 August 2019; *BBC News*, 'Norway Court Jails Mosque Gunman Manshaus for 21 Years', 11 June 2020.

III. Counterterrorist Finance and Self-Activating Terrorists

AS OUTLINED IN Chapter II, recent self-activating terrorist attacks in the EU have tended to be low cost, often without the need for substantial coordination. This has significant implications for the effectiveness of the CTF regime, which has been built on the presumption of large, complex attacks, funded by networks using the international financial system. Following the pre-existing AML approach, the CTF regime has deputised financial institutions to act as gatekeepers of that system, identifying financial intelligence and delivering it to the authorities as suspicious transaction reports (STRs).[75]

Nonetheless, the shape of the terrorist threat has evolved over the last two decades, and the regime has had mixed success in tackling terrorist financing.[76] Stakeholders within the CTF ecosystem have thus sought to reform and innovate to improve the regime's performance in detecting and disrupting terrorist activity. At EU and national government levels, AML/CTF obligations have been extended to new sectors and emerging areas of the financial system which might be vulnerable to terrorist abuse,[77] while several major European financial institutions have deployed advanced analytics to identify potential terrorists in their client book.[78] In a small number of European jurisdictions, financial institutions have also worked with law enforcement and regulators on the development of Financial Intelligence Sharing Partnerships (FISPs) to improve CTF cooperation.[79]

However, these developments – while welcome in general – have so far had a limited impact on the self-activating terrorist threat specifically. Few AML/CTF-obligated firms currently monitor transactions at a level of granularity that would allow them to detect traces of self-activating

75. 'Suspicious transaction reports' are called by a variety of names in various jurisdictions, including 'suspicious activity reports (SARs)' in the UK and the US.
76. Authors' videoconference interview with Peter Neumann, 4 May 2020; authors' videoconference interview with Nicholas Ryder, 24 April 2020; Neumann, 'Don't Follow the Money'.
77. European Commission, 'Fight Against Money Laundering and Terrorist Financing: Commission Assesses Risks and Calls for Better Implementation of the Rules', press release, 24 July 2019, <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4452>, accessed 15 April 2020.
78. Author's videoconference interview with senior compliance official from Deutsche Bank, 20 March 2020; authors' videoconference interview with senior compliance officials from HSBC, 23 April 2020; author's videoconference interviews with senior compliance officials from Lloyds Bank, 22 and 27 April 2020; authors' videoconference interviews with senior regulatory technology professional (A), 23 March 2020 and 30 April 2020.
79. Nicholas M Maxwell, 'Survey Report: Five Years of Growth in Public–Private Financial Information-Sharing Partnerships to Tackle Crime', RUSI, Future of Financial Intelligence Sharing (FFIS), August 2020.

terrorist activity and lack sufficient guidance from the public sector to fine-tune searches to be relevant to current self-activating terrorist financing typologies. Moreover, the current model does not integrate financial intelligence into the emerging investigative and preventative initiatives that are being deployed to tackle the self-activating terrorist problem. If the full value of financial intelligence is to be realised, therefore, the regime will need to find better ways to manage its identification and delivery.

The Counterterrorist Finance Regime

The current global CTF regime emerged largely in the wake of the 9/11 attacks.[80] In October 2001, the member states of the Financial Action Task Force (FATF), the international standard-setter for AML, mandated the body to expand its remit to include CTF.[81] FATF subsequently issued nine 'Special Recommendations' on CTF, which were then blended into the organisation's 40 recommendations on AML in 2012.[82] The EU, a FATF member in its own right, added CTF requirements to the third iteration of its Anti-Money Laundering Directive in 2005, [83] and updated later versions of the directive to follow FATF revisions.[84]

The FATF approach to terrorist financing has largely been based on the presumption that terrorism is a 'corporate' phenomenon, with groups fundraising through various sources – donations, legitimate businesses, criminality and state sponsorship – to support their operatives. In this model of terrorist financing, funds are transferred through the international financial system, as well as other forms of value transfer such as *hawala*, in order to help mount attacks.[85]

Based on these assumptions, the role of CTF has therefore been to identify and interdict the flow of suspicious funds, and, as with the AML regime on which it is based, it looks to financial institutions and other obligated bodies to maintain watchful surveillance of their clients and

80. Nicholas Ridley, *Terrorist Financing: The Failure of Counter Measures* (Cheltenham: Edward Elgar Publishing, 2012), p. 3; Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (London: Hachette UK, 2013), p. xiii.
81. The FATF was formed by the G7 in 1989; FATF, 'International Standards on Combating and the Financing of Terrorism and Proliferation', p. 7.
82. *Ibid*., pp. 13–30.
83. EU, 'Directive 2005/60/EC', 25 November 2005, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF>, accessed 13 August 2020.
84. EU, 'Directive (EU) 2015/849', 5 June 2015, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN>, accessed 13 August 2020; EU, 'Directive (EU) 2018/843', 19 June 2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843>, accessed 13 August 2020.
85. Authors' videoconference interview with two FATF analysts, 16 March 2020; FATF, 'Emerging Terrorist Financing Risks', October 2015, pp. 9–10; Freeman, 'The Sources of Terrorist Financing', p. 461; James Windle, 'Fundraising, Organised Crime and Financing Terrorism', in Andrew Silke (ed.), *Routledge Handbook of Terrorism and Counterterrorism* (London: Routledge, 2018), p. 195.

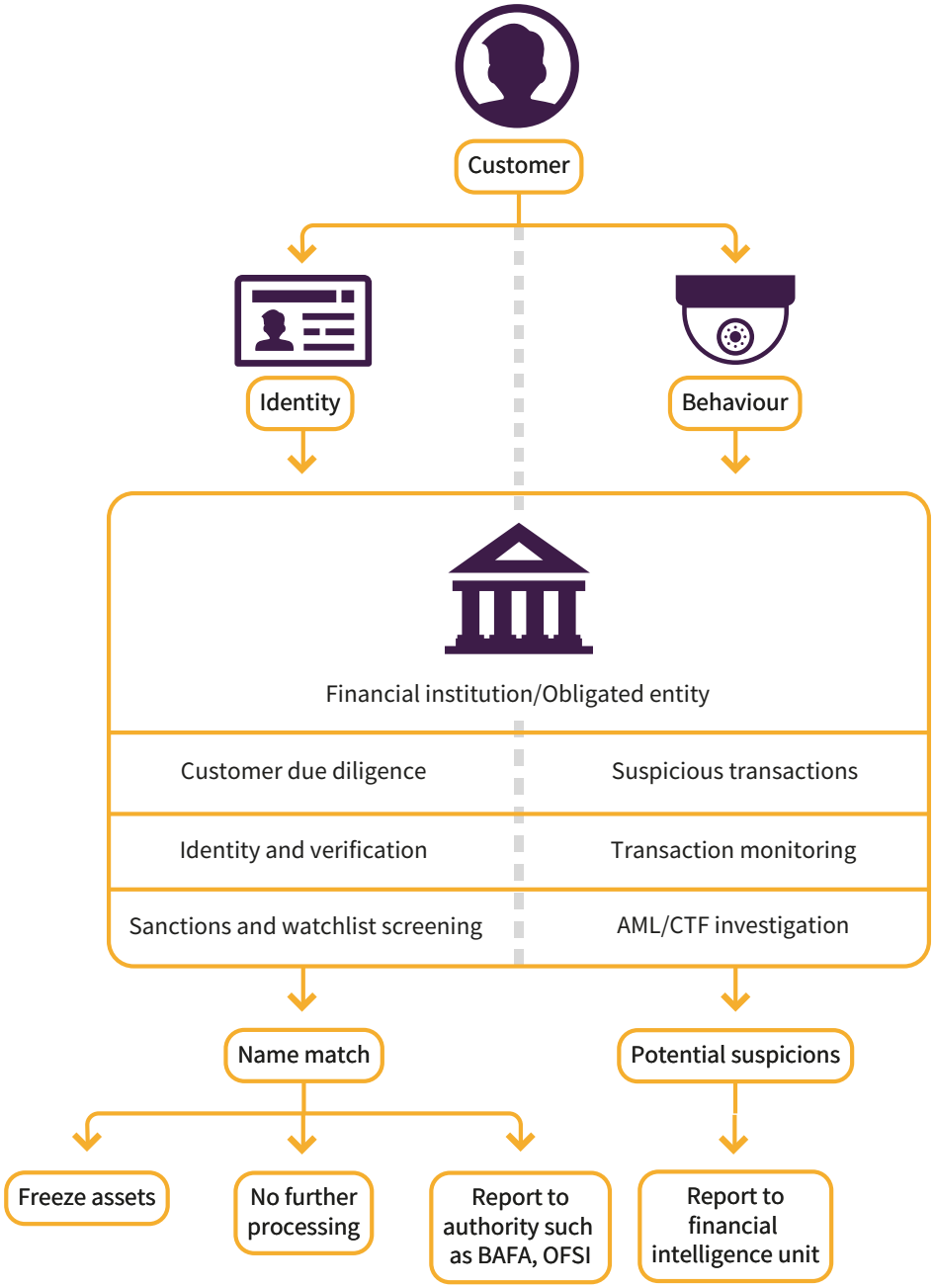
clients' activities, known as Customer Due Diligence (CDD). The requirements of CDD have evolved, but fundamentally, it has continued to comprise two essential elements:[86]

- **Prevention through identification**: Financial institutions are obligated to 'know their customers' to prevent the misuse of the financial system. When known terrorists are identified, financial institutions are expected to freeze their assets and report them to the authorities.
- **Detection through monitoring and reporting**: Financial institutions are required to undertake ongoing monitoring of clients' behaviour for potential inconsistencies with their known CDD and 'know your customer' data, as well as suspicious patterns of activity that might indicate financial crimes, including potential terrorist financing activity, and report it to national financial intelligence units (FIUs) via STRs. FIUs are then mandated to share the material with law enforcement agencies as they judge appropriate.

How the private sector should meet its obligations is left largely undefined, although it has become common over the last two decades for financial institutions to use similar frameworks, using screening platforms to identify potential name matches with sanctions or terrorist watchlists in 'real time', and transactions monitoring systems to detect potentially suspicious account activity, usually retrospectively.[87] How these two different streams of activity (identifying and monitoring) connect and feed into the wider AML/CTF system is shown in Figure 2.

86. Peter Reuter and Edwin M Truman, *Chasing Dirty Money: The Fight Against Money Laundering* (Washington, DC: International Institute of Economics, 2004), pp. 46–48.
87. Matthew Redhead, 'Deep Impact? Refocusing the Anti-Money Laundering Model on Evidence and Outcomes', *RUSI Occasional Papers* (October 2019), p. 16.

Figure 2: CTF in Practice



Source: Author generated, based on European Commission, 'Preventing Money Laundering and Terrorist Financing Across the EU: How Does it Work in Practice?', 2018, <https://ec.europa.eu/info/sites/info/files/diagram_aml_2018.07_ok.pdf>, accessed 3 January 2019; Yanan Liu and Jayant Ramen, 'Financial Crime Compliance: Current Global State of Play', Brink*, 15 October 2017, <https://www.brinknews.com/financial-crime-compliance-current-global-state-of-play/>, accessed 1 October 2020.*

Basic CTF Challenges

Terrorism researchers such as Peter Neumann and Nicholas Ryder have argued that this CTF regime has had mixed results, with terrorist groups innovating around the challenges it brings.[88] However, there are arguably more fundamental problems with the effectiveness of the regime which arise from the difficulties that the private sector has with generating useful financial intelligence.

The relative crudeness of the methods in place to identify terrorists and monitor for terrorist financing activity is a fundamental hindrance. The computer-assisted translation methods (often referred to as 'fuzzy matching') used in name screening create large amounts of false identifications, and typically only identify 'known' terrorists who have been designated under sanctions regimes or previously committed offences. Those of high concern to the authorities but not known to the private sector are usually not included in screening lists.

Transaction monitoring platforms, moreover, use rules-based approaches to look for a combination of 'red flags' in account behaviour, which mostly produce false positives. The production and investigation of alerts is also largely retrospective, with any action taking several weeks or months to result, meaning that the value of STRs as indicators of imminent attack planning can be limited.[89] Although alerts that result in STRs can often go on to provide a valuable database of post-attack intelligence, they are, however, typically of limited immediate use to the authorities when they are filed, with only 1–2% of STRs usually forming the basis of a law enforcement investigation for any type of crime.[90] Indeed, there was considerable scepticism among officials interviewed for this study about the value that STRs brought to CTF. One former long-serving senior UK police officer commented that he had 'never' seen an STR 'which led to a terrorist financing investigation', a view also expressed by Swedish and Dutch officials.[91]

There are multiple problems with transaction monitoring systems which affect their ability to detect patterns of crime. Financial institution compliance teams often lack precision in their monitoring, and commonly use combinations of red flags, or 'typologies', that are quite basic,

88. Authors' videoconference interview with Peter Neumann, 4 May 2020; authors' videoconference interview with Nicholas Ryder, 24 April 2020; Neumann, 'Don't Follow the Money', p. 101; Ridley, *Terrorist Financing*, p. 208.
89. Author's videoconference interview with senior compliance official from Deutsche Bank, 20 March 2020; authors' videoconference interview with senior compliance officials from HSBC, 23 April 2020; author's videoconference interviews with senior compliance officials from Lloyds Bank, 22 and 27 April 2020; authors' videoconference interview with a senior regulatory technology professional (B), 29 April 2020.
90. Redhead, 'Deep Impact?', p.16.
91. Authors' videoconference interviews with former senior UK law enforcement official, 14 May 2020 and 4 June 2020; authors' videoconference interview with Swedish financial intelligence unit (FIU) analyst, 3 July 2020; author's videoconference interview with former Dutch law enforcement official, 3 June 2020.

such as the receipt of funds from high-risk jurisdictions, or the international movement of large or structured amounts.[92] The platforms also typically have a poor level of resolution to detect detail, which is a challenge given the relatively small scale of much terrorist financing activity.[93] Compliance teams also apply value thresholds to the systems to prevent them becoming overwhelmed with large numbers of low-value alerts.[94]

Access to contextual material is an additional problem for financial institutions, which only have assured access to their own financial and client data. Judgements about whether a transaction is suspicious or not can depend on information held by other financial institutions, or alternative sources.[95] This is most obviously the case in CTF with secret material, which might, if available, turn a financial institution's assessment of an innocuous transaction into something more concerning.[96]

Although these aforementioned difficulties perhaps imply that poor-quality reporting is one of the reasons why STRs are not more widely exploited by the authorities, this is not always the case – even higher-quality reporting can end up having little impact if it is deemed irrelevant to current law enforcement investigations. The majority of STRs are not proactively distributed by FIUs and remain in their databases awaiting later searches by law enforcement.[97]

Distribution is not just an issue within law enforcement, moreover, as other departments with counterterrorism responsibilities – especially intelligence agencies – do not receive these reports as standard. Such agencies do of course use financial intelligence in counterterrorism investigations, but this is collated on a case-by-case basis, with legally sanctioned requests to financial institutions for information on specific individuals already under investigation. On the whole, intelligence remains largely 'walled off' from the production of CTF financial intelligence in the private sector.[98]

---

92. Author's videoconference interview with senior compliance official from Deutsche Bank, 20 March 2020; authors' videoconference interview with senior compliance officials from HSBC, 23 April 2020; author's videoconference interviews with senior compliance officials from Lloyds Bank, 22 and 27 April 2020; authors' videoconference interviews with a senior regulatory technology professional (B), 29 April 2020.
93. Authors' videoconference interview with a senior regulatory technology professional (B), 29 April 2020.
94. Matthew Redhead, 'The Future of Transaction Monitoring: Better Ways to Detect Financial Crime', SWIFT Institute Working Paper, March 2021, p. 18.
95. *Ibid*., p. 25.
96. Authors' videoconference interview with former senior UK law enforcement official, 4 June 2020; author's videoconference interview with former UK intelligence officer, 20 May 2020.
97. Authors' videoconference interview with former senior UK law enforcement official, 4 June 2020; authors' videoconference interview with Swedish FIU analyst 3 July 2020; author's videoconference interview with former Dutch law enforcement official, 3 June 2020.
98. Authors' videoconference interview with former senior UK law enforcement official, 4 June 2020; author's videoconference interview with former UK intelligence officer, 20 May 2020; author's

The Self-Activating Terrorist Problem

These problems with the delivery of actionable intelligence are especially acute in the case of self-activating terrorists. Screening systems that seek to match client and counterparties' names with sanctions and terrorist watchlists only identify significant individuals associated with proscribed or designated groups, and most self-activating terrorists, by contrast, are not on such lists, even if already known to the authorities. The generic CTF 'red flags' focusing on large amounts and foreign transactions used in transaction monitoring are also largely irrelevant to self-activating terrorists. Evidence outlined in the previous chapter suggests that self-activating terrorists are peripheral figures with modest financial means, funded domestically through licit means, such as wages and state benefits, as well as petty criminality. Although their activities should elicit concern, they typically fall outside the parameters of current monitoring.[99] Indeed, self-activating terrorists' attack planning is particularly difficult to see when monitoring platforms are not configured to distinguish between where the funds are being used, such as Amazon or eBay, and what items are being purchased. With self-activating terrorists, *what* is being bought is usually more significant than *who* is doing the selling.

The Evolving Counterterrorist Finance Regime

Since its inception, the fundamentals of the CTF regime have remained the same, although the framework has been extended and developed over time. FATF and its members' main approach has been to apply pre-existing AML/CTF obligations to a growing number of sectors which they assess might be vulnerable to criminal and terrorist abuse. Most recently this has included virtual asset service providers, such as cryptocurrency exchanges.[100]

A further governmental approach has been to identify and close loopholes after terrorist events. In the wake of the November 2015 attacks in Paris, for example, the French authorities placed tighter restrictions on the use of pre-paid cards – products which had been used by the

---

videoconference interview with former Dutch law enforcement official, 3 June 2020; authors' videoconference interview with Swedish Security Service officials, 2 July 2020.

99. Author's videoconference interview with senior compliance official from Deutsche Bank, 20 March 2020; authors' videoconference interview with senior compliance officials from HSBC, 23 April 2020; author's videoconference interviews with senior compliance officials from Lloyds Bank, 22 and 27 April 2020; authors' videoconference interviews with senior regulatory technology professional (A), 23 March 2020, 30 April 2020; authors' videoconference interview with senior regulatory technology professional (B), 29 April 2020.

100. FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', June 2019. France has recently imposed strict 'know your customer' requirements on all virtual asset service providers, citing evidence that cells in the country have financed themselves using cryptocurrencies in the past. See Danny Nelson, 'France Declares War on Crypto Anonymity, Cites "Terrorism" in KYC Mandate', *Coindesk*, 9 December 2020, <https://www.coindesk.com/france-kyc-crypto>, accessed 5 January 2021.

attackers, and similar restrictions were reflected in the EU's fifth version of the Anti-Money Laundering Directive, which came into effect in July 2018.[101]

Financial Service Innovation

Alongside governments, leading European financial institutions have also sought new ways to approach CTF. In the last decade, financial institutions have recruited many former law enforcement, military and intelligence staff, often with backgrounds in counterterrorism, into financial crime compliance and risk-management functions.[102] Although this recruitment surge has not been specifically CTF focused, it has had an impact on the devotion of resources within financial institutions, with erstwhile government professionals taking a greater interest in the investigation of networked or national security-related threats.[103] This has encouraged several European banks to undertake proactive analytic and investigative work in recent years on headline CTF issues, especially on travel to and from the Middle East by Europe-based foreign terrorist fighters.[104] Much of this work has involved the use of new tools, such as machine learning algorithms and social network analysis, to find patterns and relationships in bulk client data. Machine learning is also being used to improve the performance of existing AML/CTF controls such as screening and transaction monitoring, making it easier to categorise known patterns of suspicious behaviour with greater accuracy and speed than before.[105]

Financial Intelligence Sharing Partnerships

This growing interest in improving CTF in both the public and private sectors has also led to efforts to address this problem through FISPs. What these arrangements mean in practical terms is the sharing of strategic and typological intelligence by law enforcement agencies with the financial services sector to help them fine-tune their AML/CTF controls and provide frameworks for rapid intelligence sharing about suspects in the wake of attacks. Nine European countries

101. Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme, 'Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France', September 2019, pp. 58–59, <https://www.economie.gouv.fr/files/files/directions_services/tracfin/analyse-nationale-des-risques-lcb-ft-en-France-septembre-2019.pdf>, accessed 5 January 2021; EU, 'Directive (EU) 2018/843'.
102. Redhead, 'Deep Impact?', p. 27.
103. Authors' videoconference interview with senior compliance officials from Lloyds Bank, 27 April 2020; authors' videoconference interview with senior compliance officials from HSBC, 23 April 2020.
104. Author's videoconference interview with senior compliance official from Deutsche Bank, 20 March 2020; authors' videoconference interview with senior compliance officials from HSBC, 23 April 2020; author's videoconference interviews with senior compliance officials from Lloyds Bank, 22 and 27 April 2020; authors' videoconference interviews with senior regulatory technology professional (A), 23 March 2020, 30 April 2020.
105. Authors' videoconference interview with senior regulatory technology professional (B), 29 April 2020.

have a FISP in place, and of those, seven have so far prioritised terrorist financing as a key area for cooperation.[106]

However, most EU members have not followed this route, and in the case of France, the government has taken an alternative approach to financial intelligence sharing. Since 2015, France has mandated Tracfin, the country's FIU, to directly monitor the financial activities of individuals on the French Interior Ministry's database of known terrorists, criminals and suspects.[107] Although this does not remove financial institution and other AML/CTF obligations, it does provide the French authorities with direct financial insights into the activities of individuals already of concern.

Impact of Counterterrorist Finance Reform

The value of these changes for overall CTF performance is hard to quantify. Although extending the existing rules to new areas of activity as threats emerge is a necessary step, this is a never-ending process, because all terrorists, including self-activating terrorists, exhibit fluidity and versatility in their financial behaviour. As a French official noted in an interview, the kinds of consumer loans exploited by Coulibaly were an attractive terrorist financing typology in France, but following the imposition of tighter controls following his attack, terrorists shifted towards unregulated spaces online, or criminality.[108] Changes in the rules had led to a displacement of activity, not its elimination.

Nonetheless, practitioner views of the impact of private sector innovation has been broadly positive. Although the use of advanced technologies by financial institutions to detect shifts in behaviour or unusual patterns is still in its relative infancy, many in the private sector believe it has the potential to generate new financial intelligence of potential CTF value, especially if informed by law enforcement and intelligence agencies advice on up-to-date typologies.[109] The

106. Jurisdictions with financial intelligence-sharing partnerships are Austria, Finland, Germany, Ireland, Latvia, Lithuania, Sweden, Netherlands, and the UK. Of these only Austria and Germany do not prioritise CTF. See Maxwell, 'Survey Report', pp. 28–50.
107. Michael Stothard, 'France Seeks New Powers to Monitor Terror Suspects' Bank Accounts', *Financial Times*, 23 November 2015; authors' videoconference interview with French FIU analysts, 10 September 2020.
108. Author's videoconference interview with former French FIU analyst, 30 June 2020.
109. Author's videoconference interview with senior compliance official from Deutsche Bank, 20 March 2020; authors' videoconference interview with senior compliance officials from HSBC, 23 April 2020; author's videoconference interviews with senior compliance officials from Lloyds Bank, 22 and 27 April 2020; authors' videoconference interview with former senior UK law enforcement official, 4 June 2020; author's videoconference interview with former UK intelligence officer, 20 May 2020; author's videoconference interview with former Dutch law enforcement official, 3 June 2020.

available data on the value coming from FISPs is encouraging. In the Netherlands, for example, the terrorist financing-dedicated FISP, the Netherlands Terrorism Financing Taskforce, made 300 case-specific reports between July 2017 and June 2019, which contained 6.4 times the amount of disclosable intelligence than an average terrorist financing-related STR.[110] Nonetheless, as a result of their limited scale, FISPs have so far only been able to focus on a relatively small number of high-profile investigations. In the Netherlands, the FIU received nearly 2.5 million STRs in 2019 alone,[111] of which the 300 aforementioned cases are a tiny proportion.

Counterterrorist Finance Reform and Self-Activating Terrorists

It is more difficult still to clarify what impact these changes have had on tackling the self-activating terrorist threat, and practitioners were sceptical about the CTF regime's potential to address the issue without radical reform. As one Swedish official commented in an interview, the CTF regime's limited capacity to provide useful pre-attack financial intelligence was 'a feature, not a bug'.[112]

In the UK, the sharing of typological information specifically on self-activating terrorist attacks through the Joint Money Laundering Intelligence Taskforce has aided a number of major financial institutions in undertaking speculative analytic work around the problem.[113] Major financial institutions in France and Germany have also carried out similar kinds of analytic work on self-activating terrorists.[114] However, there is no publicly available information to assess whether the material produced has had a positive effect, and there are indications that because these private sector analyses are based on assessments of 'risk', rather than the legal standard of 'suspicion', they can often sit unexploited by the authorities, even where FISPs exist.[115] Although this is a problem caused by current AML/CTF laws, it is reinforced by Article 7 of the EU's General

110. Maxwell, 'Survey Report', p.20.
111. FIU-The Netherlands, 'Annual Review: 2019', p. 31, <https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/fiu-nederland_jaaroverzicht_2019_en_0.pdf>, accessed 20 August 2020.
112. Authors' videoconference interview with Swedish FIU analyst, 3 July 2020.
113. Authors' videoconference interview with UK-based regulatory technology firm, 29 April 2020; authors' videoconference interview with Israel-based regulatory technology firm, 30 April 2020; authors' videoconference interview with senior compliance official from Lloyds Bank, 27 April 2020; authors' videoconference interview with senior compliance officials from HSBC, 23 April 2020.
114. Author's videoconference interview with senior compliance official from Deutsche Bank, 20 March 2020; authors' videoconference interviews with senior regulatory technology professional, 23 March 2020 and 30 April 2020.
115. Authors' videoconference interview with senior compliance officials from Lloyds bank, 22 April 2020, 27 April 2020; authors' videoconference interview with senior compliance officials from HSBC, 23 April 2020.

Data Protection Regulation, which prohibits the sharing of information on individuals without consent unless, according to Article 29, it is in the 'public interest'.[116]

Evidence is better for the role that FISPs can play in real-time intelligence sharing on self-activating terrorists post-incident, where financial institutions have supported investigations in ad hoc public–private 'fusion cells'.[117] Several major financial institutions noted their roles in such efforts, and public sector investigators confirmed the value of their contributions with real-time intelligence relating to purchases, CDD materials, and identification of additional suspects through transactions data. When interviewed, a senior Dutch official noted how valuable financial intelligence transmitted via FISP arrangements had been in locating the suspect in the Utrecht tram shooting of March 2019.[118]

Nonetheless, this kind of sharing has limited impact on the proactive work of intelligence agencies and police in preventing such attacks, apart from the identification of extremist associates through financial links, who might themselves become future self-activating terrorists. With CTF FISPs primarily focused on high-priority and strategic concerns, the day-to-day operational machinery needed to share such information at scale for known but lower-priority targets does not therefore exist in most jurisdictions, except perhaps in France, where Tracfin is already directly monitoring the financial activities of a wide range of known terrorist suspects.

FISP arrangements also have no apparent link to preventative counterterrorism interventions specifically designed to tackle the self-activating terrorist threat at source. In Sweden, the security agency SÄPO works closely with many elements of the public sector – social services, health, education – to identify those at risk, especially with mental health issues.[119] In recent years, the UK has also widened the scope of its counterterrorism approach further, with the creation of local 'multi-agency centres', where the police and intelligence agencies work with health, education and welfare departments, mutually sharing information about individuals of concern in a secure and vetted environment.[120] However, these programmes chiefly involve public sector agencies and civic bodies rather than private sector intelligence providers such as financial institutions, or social media. Based on past cases, there are reasonable grounds to suppose that the addition of material from such providers would provide potentially useful intelligence on a vulnerable person's activities.

The Way Forward

In spite of attempts to improve the CTF regime, therefore, methods of CTF financial intelligence collection and distribution remain crude and unguided, causing particular problems for tackling

116. GDPR.EU, 'General Data Protection Regulation', <https://gdpr.eu/tag/gdpr/>, accessed 24 February 2021.
117. Authors' videoconferencing interview with senior compliance officials from HSBC, 23 April 2020.
118. Author's videoconference interview with former Dutch FIU official, 3 June 2020.
119. Authors' videoconference interview with Swedish Security Service officials, 2 July 2020.
120. Home Office, *CONTEST: The United Kingdom's Strategy for Countering Terrorism* (London: The Stationery Office, June 2018), p. 42.

the self-activating terrorist threat. This is a frustrating situation, however, because it is apparent that self-activating terrorists do create financial traces, but these are not being translated into exploitable intelligence for the authorities. CTF is taking steps in the right direction with the development of FISPs, but these arrangements remain several steps away from being likely to generate an impact on self-activating terrorists. Looking at wider counterterrorism efforts, it appears that more extensive real-time cooperation between intelligence, law enforcement and 'non-traditional' partners such as financial institutions might be a more effective way to bridge that gap.

Conclusion and Recommendations

SELF-ACTIVATING TERRORIST ATTACKS are a persistent threat in Europe, although not one typically considered from the perspective of terrorist financing. This paper has sought to start building a better evidence base on self-activating terrorist financial behaviours in attack planning and assess how effective current CTF controls have been in detecting them. The study has prompted a range of findings – and potential options for future action – outlined in this section.

Self-Activating Terrorist Financial Behaviours

The existing academic literature on the terrorist financing dimensions of self-activating terrorist activity is limited, and interviews with law enforcement officers and other counterterrorism officials have revealed a widespread assumption that there are few meaningful financial dimensions to the cases to consider.

The majority of self-activating terrorist attacks covered in this study have indeed been relatively small in scale and exhibited low levels of sophistication. The most common remains one which uses a sharp-edged item such as a knife, which is easily accessible in domestic settings. However, because such weapons *can* be easily sourced without financial activity, does not mean that they *are*. The study has found examples of self-activating terrorists specifically buying edged weapons for the purpose of an attack, sometimes in mainstream retail settings, or from specialist merchandisers. These actions can leave a trace.

Other forms of self-activating terrorist attack planning can also leave financial footprints. Unless stolen, vehicles or firearms have to be paid for, even when sourced through criminal means. Preparations for IED attacks, which involve the procurement of a range of different components, will also involve considerable financial and commercial activity, as the cases of the 2019 Lyon bomber, Mohamed Hichem Medjoub, or the Abedi brothers in Manchester, indicate.

Key Finding 1: Self-activating terrorist attack planning can have a financial and commercial dimension that is not as yet fully appreciated by practitioners.

- **Recommendation 1**: It is vital that Europol, Eurojust and other relevant EU-level agencies should work with member states' law enforcement and intelligence agencies on the collection and analysis of sensitive and publicly unavailable financial and commercial information in self-activating terrorist cases, to create an evidence-based understanding of attack-planning behaviours and a library of typologies that could provide financial institutions with a better understanding of the logistics of self-activating terrorist events.

A further common assumption is that any self-activating terrorist financial activity is largely invisible, carried out in cash, or beyond the world of conventional finance, in emerging financial technologies (such as cryptocurrencies). This study suggests that cash does indeed play a significant role but it is mixed in with digital transactions which leave more indelible marks. Some self-activating terrorists have used financial products outside the 'legacy' banking system, such as dedicated payment service providers and, in a small number of cases, cryptocurrencies, but this continues to be mixed in with services from traditional providers, including high-street banks.

Key Finding 2: Self-activating terrorists' financial activity is not necessarily negligible or invisible, and attackers use a range of financial channels and products, including cash, digital payments and in a small number of cases, financial technologies, to undertake their activities.

- **Recommendation 2a**: The private sector and EU agencies have better prospects of tracing suspicious activity where cash is not used. The European Commission should therefore review the potential benefits of limiting cash payments (or requiring customer identification and verification) in the purchase of a small number of types of high-risk items such as ornamental or ritualistic edged weapons, or chemicals used in IEDs.
- **Recommendation 2b**: In keeping with its wider AML/CTF responsibilities, the European Commission should undertake an *annual* review with relevant EU agencies to ensure that its Anti-Money Laundering Directives cover all relevant emerging financial technologies and platforms that might be used by criminals and terrorists.

A further notable dimension of the cases reviewed are the significant levels of interaction between self-activating terrorists and 'universal' online retailers such as Amazon and eBay, especially with regard to the procurement of IED components. Although not strictly linked to terrorist financing *per se*, it is clear that such sites play an important role as potential suppliers to self-activating terrorists and collate significant amounts of data on the financial activities of their customers and therefore on the potential logistics of attack planning by some self-activating terrorists.

Key Finding 3: The economic ecosystem that self-activating terrorists (and terrorists in general) currently operate within is broad, and their financial activities also leave commercial traces with regard to the purchase of high-risk items. There is currently no requirement for commercial institutions to monitor, identify or report potentially suspicious terrorist financing-linked purchases.

- **Recommendation 3a**: The European Commission should consider the development of a list of 'high-risk' items that could be used in self-activating terrorist attacks, to guide vendor decisions on whether to execute a sale.
- **Recommendation 3b**: The European Commission should review whether specific types of retail outlet which sell high-risk items should be encouraged to develop voluntary reporting mechanisms of suspicious items or be covered by mandatory AML/CTF monitoring and reporting requirements.

Counterterrorist Financing Effectiveness and Self-Activating Terrorists

As noted in the previous chapter, the current CTF regime is focused primarily on the detection of terrorist financing linked to known terrorist groups. The onus is placed on financial institutions and other obligated firms to identify potential terrorist customers or counterparties, to freeze accounts, and to report financial intelligence to FIUs for the use of law enforcement.

The impact of this approach has been mixed overall, partly because of its relative inflexibility in the face of a changing terrorist threat. More fundamentally, it places heavy reliance on financial institutions having the knowledge and technological capacity to detect appropriate financial intelligence, and a bureaucratic process effectively delivering and distributing that financial intelligence within the public sector. These basic CTF challenges are extremely acute for self-activating terrorists, because screening tools will only detect known terrorists, and transaction monitoring tools are usually not calibrated to detect behaviours which might indicate self-activating terrorist activity.

Key Finding 4: CTF faces basic problems with the detection of financial intelligence because of its focus on outdated models of terrorist financing, problems which are exacerbated in small-scale but complex problems such as self-activating terrorists.

- **Recommendation 4**: The European Commission and relevant EU agencies should consult on ways to ensure financial institutions and other obligated entities produce better and more timely financial intelligence on self-activating terrorists. This could include:
    - The development of evidence-based self-activating terrorist typologies, case studies and supporting information (based on work in Recommendation 1) to be shared with member states' governments and agencies, and the AML/CTF obligated private sector.
    - Feasibility studies on how AML/CTF transaction monitoring platforms can best exploit modern payments data to provide a more granular view of client activity, and how new technologies could be used to get institutions closer to 'real-time' monitoring for threat-to-life risks.

A further issue for CTF has been the delivery of financial intelligence to appropriate elements in the public sector. This is often attributed to problems with STR quality – in other words, a perception that STRs are not necessarily useful enough to be worth distribution. But this is not always the case, and good material goes unused either because it is deemed irrelevant to law enforcement investigations or it is not distributed to other stakeholders in the counterterrorism community.

Key Finding 5: Where the private sector does provide well-prepared CTF financial intelligence, it is often poorly aligned to investigative priorities, or poorly distributed, and therefore goes unexploited.

- **Recommendation 5**: The European Commission and relevant EU agencies should consult on ways in which CTF financial intelligence can be better aligned with current risk priorities and distributed to all relevant audiences. This could include:
    - The development of prioritisation and feedback mechanisms for CTF STRs between the public and private sector. Responsible public agencies could set specific requirements for the kind of financial intelligence they wish to receive (such as potential self-activating terrorist activity) and provide evaluations of whether those requirements are being met.
    - The requirement that all counterterrorism-tasked intelligence services should become standard and integral elements in the distribution and feedback channels of CTF-related STRs.

In the face of a variety of problems, the CTF regime has evolved both through policy direction and organic innovation over recent years. Governments have expanded the scope of the AML/CTF regime and financial institutions have deployed new investigative talent and analytic technologies on proactive, risk-focused projects. Both the public and private sector have also begun to work together in several jurisdictions on specific CTF-focused FISPs, or, in the case of France, direct public sector transactions monitoring.

However, proactive work in the private sector that might generate individual leads does not get shared between the public and private sectors, because of reporting and data-sharing restrictions around individuals' personal information. Although this has not stopped private sector work on the self-activating terrorist problem, it has limited its wider exploitation.

Key Finding 6: Current lead-generating initiatives that have the potential to identify potential financial intelligence on self-activating terrorists have not been fully encouraged or exploited by the public sector.

- **Recommendation 6a**: The European Commission and relevant EU agencies, in particular Europol and the EU's proposed new AML/CTF regulatory authority, should encourage national law enforcement agencies and regulators, and by extension the private sector, to exploit new technologies and data analytics in general, and on the self-activating terrorist problem in particular. Ideally, this should be in collaborative environments such as FISPs.
- **Recommendation 6b**: The European Commission should consider how to support such collaborations through a review and potential extension of the legal thresholds for sharing CTF data in AML/CTF and data-protection law.

Current CTF work is also hindered by the bureaucratic character of existing partnerships. The periodic, meeting-based structure of most FISP arrangements does not allow for 'real-time' intelligence sharing apart from *after* an attack. FISPs also focus on known, high-risk targets,

rather than the lower-priority or unknown individuals who often become self-activating terrorists. In several jurisdictions, moreover, potential self-activating terrorists are now the focus of localised preventative interventions, pooling intelligence from across the public sector, but not – it appears – financial intelligence or other kinds of private sector intelligence.

Key Finding 7: Current CTF collaborations are not structurally flexible or wide-ranging enough to tackle the self-activating terrorist problem proactively.

- **Recommendation 7**: The European Commission and relevant EU-level agencies should review the options for more flexible and agile CTF intelligence sharing to aid proactive self-activating terrorist identification. This could include reviewing the likely costs and operational benefits of:
    - Direct data sharing/transaction monitoring for CTF risks by a government agency, such as in France, or potentially in collaboration with the private sector.
    - The development of private–public sector intelligence 'fusion cells' to create real-time intelligence sharing on CTF issues such as potential self-activating terrorists.

Assessing the Costs

It is likely that such reviews will indicate the need for additional public sector and/or private sector investment to support such options, prompting basic practical questions of 'who pays?'. Limitations on realistic public expenditure need to be taken into account. If these options are to be explored – especially in Recommendation 7 – potential models for financial burden-sharing between the sectors will also need to be reviewed, such as the UK's proposed levy on UK banks to support an expanded government response to economic crime.[121]

Calls for reform that necessitate greater investment also raise issues of financial proportionality, especially in light of the relatively limited human and economic impact of most self-activating terrorist attacks in comparison with large-scale attacks coordinated by terrorist groups. Whether governments believe that these investments bring a worthwhile return in reducing the numbers of such attacks also carries political and ethical assumptions and it is difficult in a paper such as this to recommend where to strike the balance. Although this paper does not make a specific recommendation in this regard, the authors believe it vital that these issues are taken into consideration. Because something *can* be done does not necessarily mean it *has* to be done, especially if this brings undesired consequences.

Furthermore, some of the potential ways forward could be more intrusive, with closer surveillance of some individuals' financial activity, whether conducted by the private or public sector, and a wider sharing of that information, likely to result. Again, this would generate both practical and ethical issues, given the importance of civil liberties in European societies. If financial institutions were to work more closely with law enforcement and intelligence agencies on the monitoring

121. HM Treasury, *Economic Crime Levy: Funding New Government Action to Tackle Money Laundering* (London: The Stationery Office, 2020).

of some individuals of potential terrorist concern, appropriate safeguards have to be in place; at the very least the use of secure systems and the vetting of relevant private sector staff, validated by the public sector agencies with which the financial institutions are collaborating. Technological workarounds such as encrypted privacy-enhancing technologies might allow the public sector to monitor the financial activities of such individuals remotely without revealing their subjects of interest to financial institutions or their staff.[122]

122. Nick Maxwell, 'Future of Financial Intelligence Sharing (FFIS): Innovation and Discussion Paper: Case Studies of the Use of Privacy Preserving Analysis to Tackle Financial Crime', RUSI/ FFIS, June 2020, pp. 9–12.

About the Authors

Stephen Reimer is a Research Fellow at RUSI's Centre for Financial Crime and Security Studies.

Matthew Redhead is a writer on issues relating to national security, intelligence and financial crime. In 2018, he became an Associate Fellow at RUSI in the Financial Crime 2.0 programme. He worked as a financial crime risk professional at a major global bank for seven years, and as a financial crime consultant to the FinTech and RegTech sectors. He has also served as a government official at the UK Home Office and Ministry of Defence.

Annex

The table below provides details on the 106 self-activating terrorist cases identified in a review of English language reporting from mainstream national print and broadcast media from all in-scope countries over the period of study (January 2015 and November 2020). Divided by country, the table indicates the number of plots perpetrated by one ('Solo'), two ('Dyad') or three ('Triad') individuals and the ideological motivation for the attack, either Islamist extremism ('Isl/Ex') or far-right extremism ('Xrw'). The table also provides a breakdown of the weapons used in these attacks, including blunt weapons ('Blunt weapon'), edged weapons such as knives or swords ('Edged weapon'), firearms or guns ('Firearm'), improvised explosive devices or bombs ('IED'), vehicles used for attacking victims ('Vehicle'), and biochemical weapons ('Biochem'). Cases involving any combination of the other weapon types are logged under the last column ('Combo').

Figure 3: Aggregate Figures of Cases Reviewed Within Relevant Jurisdictions Between January 2015 and November 2020

Jurisdiction	Cases	Self-Activating Terrorist Cell Size			Ideology		Weapon Type						
		Solo	Dyad	Triad	Isl/Ex	Xrw	Blunt weapon	Edged weapon	Firearm	IED	Vehicle	Biochem	Combo
France	35	33	1	1	35	0	1	17	5	2	6	0	4
UK	25	20	4	1	18	7	0	9	0	8	2	0	6
Germany	21	17	1	3	13	8	0	7	4	5	2	1	2
Sweden	4	4	0	0	3	1	0	1	0	1	2	0	0
Austria	1	1	0	0	1	0	0	0	0	0	0	0	1
Croatia	1	1	0	0	0	1	0	0	1	0	0	0	0
Italy	3	3	0	0	2	1	0	1	1	0	1	0	0
Demark	3	2	1	1	3	0	0	0	1	2	0	0	0
Norway	1	1	0	0	0	1	0	0	1	0	0	0	0
Poland	2	1	0	0	1	1	0	1	0	1	0	0	0
Finland	1	1	0	0	1	0	0	1	0	0	0	0	0
Lativa	1	1	0	0	0	1	0	0	0	0	0	0	1
Netherlands	4	3	1	0	4	0	0	2	1	1	0	0	0
Belgium	4	4	0	0	4	0	0	2	0	1	0	0	1
Total	**106**	**92**	**8**	**6**	**85**	**21**	**1**	**41**	**14**	**21**	**13**	**1**	**15**