



The Lebanese Hizbullah Financing Threat in Europe

Matthew Levitt

About Project CRAFT

Project CRAFT 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 CRAFT is funded by the European Union'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 projectcraft.eu.

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

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



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

Hizbullah gets the majority of its funding and weapons from Iran, but the group also runs parallel independent fundraising and arms procurement efforts around the world, including in Europe, to complement its state sponsorship from Iran. These independent fundraising and procurement operations have become more pronounced over time, especially in the wake of wars that depleted weapons stockpiles and sanctions and declining oil prices which have impacted Iranian funding levels.

Background: Diversifying Hizbullah's Portfolio beyond Iranian Largesse

Despite Iran's generous sponsorship of Hizbullah, events have in the past, and are now once again, forcing the group to diversify its financial portfolio beyond Iran's generous state sponsorship. The turning point came in 2009, when Hizbullah's leaders decided to vastly expand the group's independent funding capabilities.

Following Hizbullah's 2006 war with Israel, Iran ramped up its funding to defray Hizbullah's soaring costs of restocking its weapons supplies, investing in reconstruction, and buying favour within communities that suffered damage during the war.¹ It was especially desperate for support in advance of Lebanon's June 2009 elections, as the group attempted to compete with its Sunni political rivals, who were funded by Saudi Arabia.² But even with Iranian state sponsorship, Hizbullah began to expand its reliance on its criminal-financial networks to meet its increased financial needs in the wake of the 2006 war.³

Over the next couple of years, Iran was flush with cash as oil prices rose as high as \$147 per barrel by late-July 2008.⁴ But by mid-January 2009, oil prices fell to \$36 per barrel and remained under \$60 until May.⁵ At the

same time, increased international sanctions, rampant corruption, and soaring inflation severely undermined the Iranian economy. Soon after, Tehran's ruling clerical elite blatantly stole the country's June 2009 elections, leading to the months-long Green Movement protests and forcing Iran to focus its attention inward.⁶

According to Israeli intelligence, these economic pressures forced Tehran to slash its annual budget for Hizbullah by as much as 40% in early 2009. Suddenly constrained after years of abundant Iranian funding, Hizbullah turned to its pre-existing criminal enterprises – including those in Europe – to boost its assets.⁷

Hizbullah has long engaged in a wide range of activities in Europe, from operations to logistical activities such as financing and arms procurement. Sometimes, these activities are exposed only after the fact, and even then not fully understood. For example, Hizbullah operative Hossam Yaacoub was convicted in March 2013 of engaging in an operation in Cyprus, but it was only in the course of that investigation that authorities learned that Yaacoub earlier served as a Hizbullah courier with journeys to France and The Netherlands. The nature of those trips to Europe, and the identities of the Europe-based Hizbullah operatives with whom he met, remain unknown.⁸ Later, authorities would learn that a French-Lebanese academic then living in France provided the funds for the purchase of a safe house in Cyprus where another Hizbullah operative stockpiled ice packs from which chemicals could be extracted to make ammonium-nitrate bombs.⁹

But what case after case demonstrates is that Hizbullah sees Europe as a land of tremendous financial opportunity, even after the 2013 EU designation of the group's terrorist and military wings – as distinct from its political or social branches, a distinction Hizbullah itself insists does not exist. In a sign of the importance Hizbullah attaches to its financial and other activities in Europe, the group

1. Nicholas Blanford, *Warriors of God: Inside Hezbollah's Thirty-Year Struggle Against Israel* (New York, NY: Random House, 2011), pp. 336–39; Alistair Lyon, 'Lebanon's Postwar Reconstruction Far from Complete', *Reuters*, 9 July 2007; 'Treasury Designates Hizballah's Construction Arm', US Treasury Department, 20 February 2007.
2. 'Iran: A Need for Budget Cuts', *Stratfor*, 13 April 2009.
3. John Fernandez, 'The DEA's Targeting of Hezbollah's Global Criminal Support Network', Policywatch 3240, The Washington Institute, 10 January 2020.
4. 'Oil Hits Record above \$147', *Reuters*, 10 July 2008.
5. US Energy Administration, 'US FOB Costs of OPEC Countries Crude Oil', 1 April 2020.
6. Robert F Worth and Nazila Fathi, 'Protests Flare in Tehran as Opposition Disputes Vote', *New York Times*, 13 June 2009.
7. Matthew Levitt, 'Hezbollah: Party of Fraud', *Foreign Affairs*, 27 July 2011.
8. Matthew Levitt, 'Hizb Allah Resurrected: The Party of God's Return to Tradecraft', *CTC Sentinel*, The Washington Institute, 29 April 2013.
9. Matthew Levitt, 'Hezbollah's Criminal and Terrorist Operations in Europe', *AJC*, 2 September 2018.

promoted one of the senior commanders for Hizbullah activities in Europe to be political advisor to Hizbullah leader Hassan Nasrallah.¹⁰

Today, Hizbullah and Iran both face significant financial stress even as they continue to deploy operatives to fight Assad's war in Syria. US officials suggest that Iran provides Hizbullah some \$700 million a year, though that is sure to fluctuate with increased sanctions and oil market disruptions.¹¹ But as Iran and Hizbullah continue to face significant financial pressure, Hizbullah will increasingly rely even more on its own independent financing schemes, including those in Europe. These can be broken down into three primary categories: criminal enterprises, businesses, and abuse of charity.

Criminal Enterprises

Hizbullah's transnational criminal enterprises have expanded to such a degree that international law enforcement agencies have partnered together to create the Law Enforcement Coordination Group, which last met in December 2019 in The Hague, as a vehicle for sharing information and best practices to counter Hizbullah's terrorist and criminal activities.¹² Complementing this effort, the US Treasury Department launched the Counter-Hizbullah International Partnership for finance ministries and financial investigators and regulators 'to build multilateral cooperation for targeting Hizbullah's global financial networks'.¹³

Following the 2006 Hizbullah–Israel war, the group engaged in a global procurement effort to restock its weapons arsenal. For example, Dani Tarraf, a German-Lebanese dual-citizen and Hizbullah procurement agent, used his Slovakian import–export

company to procure weapons for Hizbullah. US authorities determined the company, Power Express, 'operated as a subsidiary of Hizbullah's technical procurement wing'.¹⁴ But before the FBI caught him trying to purchase surface-to-air missiles for Hizbullah, Tarraf was already deeply involved in a host of money-making criminal schemes such as underwriting the purchase of stolen merchandise that Hizbullah operatives then shipped and sold around the world.¹⁵ Other Hizbullah operatives affiliated with Tarraf engaged in other crimes, such as producing and selling counterfeit euros, US dollars, and other currencies.¹⁶

Tarraf was lured to the US and arrested there. But over the past few years, Hizbullah has expanded its criminal activities in Europe, leading to the arrest of operatives engaged in money-laundering, narcotics trafficking, counterfeit currency and clothing, and other illegal schemes in countries across Europe, from Belgium and the Czech Republic, to France and Lithuania.¹⁷

In October 2015, US and French authorities collaborated to arrest two individuals, a Lebanese-French woman, Iman Kobeissi, in Atlanta and her associate, Joseph Asmar, in Paris, on charges of conspiring to launder narcotics proceeds and international arms trafficking on behalf of Hizbullah. Kobeissi was arraigned on charges for conspiracy for laundering funds she believed to be drug money, and for arranging for the sale of thousands of firearms, including military assault rifles, machine guns, and sniper rifles, to criminal groups in Iran and Lebanon, including Hizbullah. Asmar was arrested in Paris the same day and charged with money-laundering conspiracy.¹⁸ The investigation into the two Hizbullah associates effectively mapped out the extent of Hizbullah's criminal reach into and across Europe.

10. 'Treasury and the Terrorist Financing Targeting Center Partner Together to Sanction Hizbullah's Senior Leadership', US Treasury Department, 16 May 2018.
11. Nathan Sales, 'Tehran's International Targets: Assessing Iranian Terror Sponsorship', The Washington Institute, 13 November 2018.
12. 'Eighth Meeting of the Law Enforcement Coordination Group Focused on Countering Hizbullah's Terrorist and Illicit Activities', Office of the Spokesperson, US State Department, 17 December 2019.
13. 'Treasury Launches the Counter-Hizbullah International Partnership (CHIP) to Thwart Illicit Financial Activity', US Treasury Department, 18 October 2019.
14. Matthew Levitt, 'Hezbollah's Procurement Channels: Leveraging Criminal Networks and Partnering with Iran', *CTC Sentinel* (Vol. 12, No. 3, March 2019).
15. US vs. Dani Nemr Tarraf et al, Indictment and Criminal Complaint, Crim. No. 09-743-01, US District Court, Eastern District of Pennsylvania, 20 November 2009.
16. US vs. Hassan Hodroj et al, Indictment, United States District Court, Eastern District of Pennsylvania, 24 November 2009, <https://www.investigativeproject.org/documents/case_docs/1137.pdf>, accessed 8 April 2020.
17. Fernandez, 'The DEA's Targeting of Hezbollah's Global Criminal Support Network'.
18. 'Two Hezbollah Associates Arrested On Charges Of Conspiring To Launder Narcotics Proceeds And International Arms Trafficking', US Attorney's Office Eastern District of New York, US Department of Justice, 9 October 2015.

According to the Department of Justice, ‘Kobeissi and Asmar explained that they could arrange for planes from South America laden with multi-ton shipments of cocaine to land safely in Africa as a transit point before the drugs were smuggled to the US or Europe’.¹⁹ In conversations recorded by law enforcement, the two discussed their money-laundering network and the transportation and banking services they provided to drug traffickers, terrorist organisations, and other criminal groups in Lebanon, Iran, France, Belgium, Bulgaria, Benin, the Democratic Republic of the Congo, Ghana, Nigeria, Cyprus, and cities across the US.²⁰

The investigation caught Kobeissi and Asmar laundering drug proceeds through Europe and seeking to purchase cocaine and weapons there, specifically for ‘Hizbullah and other independent criminal groups in Iran’.²¹ According to court documents, they also offered to use ‘Hizbullah-connected associates’ to provide security for narcotics shipments.²² One of these Hizbullah associates, located in the UK, laundered £30,000 for a US Drug Enforcement Administration undercover agent posing as a narcotics trafficker. The UK-based Hizbullah associate also discussed distribution of cocaine shipments with the undercover agent and requested to purchase kilogram quantities of cocaine.

In another case, Colombia-based Hizbullah associate Mohammad Ammar was arrested in the US in October 2016 for laundering narcotics proceeds through Miami banks.²³ A British citizen (who reportedly also holds Lebanese, Canadian, and American citizenship), Ammar ‘is known for facilitating the laundering of illicit monies from or through Holland, Spain, the UK, Australia and Africa’, according to US court documents.²⁴ Another associate was arrested in France, and a third remains a fugitive, thought to be hiding in Lebanon or Nigeria.

Then, in February 2016, investigations by US and European law enforcement led to the revelation that Hizbullah’s

terrorist wing, the External Security Organisation (also known as the Islamic Jihad Organisation), runs a dedicated entity specialising in worldwide drug trafficking and money laundering. This finding was uncovered through Operation Cedar, a joint operation that included several US law enforcement agencies working in concert with Europol, Eurojust, and authorities in France, Germany, Italy, and Belgium. The investigation spanned seven countries and led to the arrest of ‘top leaders’ of a Hizbullah ‘European cell’ on charges of drug trafficking, money laundering, and procuring weapons for Hizbullah’s use in Syria.²⁵

These included Mohamad Nouredine, ‘a Lebanese money launderer who has worked directly with Hizbullah’s financial apparatus to transfer Hizbullah funds’ through his companies while maintaining ‘direct ties to Hizbullah commercial and terrorist elements in both Lebanon and Iraq’.²⁶ The US Treasury had already designated Nouredine and his partner, Hamdi Zaher El Dine, as Hizbullah terrorist operatives in January 2016, noting that the group needs individuals like these ‘to launder criminal proceeds for use in terrorism and political destabilization’.²⁷ This was no rogue operation but, rather, a function of Hizbullah’s ‘financial apparatus’, which ‘maintained direct ties’ to both Hizbullah commercial and terrorist elements.²⁸

According to information the German Ministry of Interior provided the German Parliament, four of the suspects arrested in Operation Cedar were in Germany and some of the early evidence leading to the operation came from Customs investigations into two Lebanese cash couriers who were bringing cash into Germany to purchase luxury goods as a means of laundering the proceeds of Hizbullah criminal activities. While Hizbullah sees Germany as a comfortable place to operate, the Ministry of the Interior informed parliament that the domestic intelligence service does keep certain entities, including the Islamic Center Hamburg, under observation. Moreover, federal

19. *Ibid.*

20. *Ibid.*

21. *Ibid.*

22. *Ibid.*

23. David Ovalle, ‘State: Hezbollah-Linked Group Laundered Drug Money through Miami Banks’, *Miami Herald*, 11 October 2016.

24. Mark Schliebs, ‘Australia Terrorist Money-Laundering Links to Drug Cartels’, *The Australian*, 2 November 2016.

25. ‘DEA and European Authorities Uncover Massive Hizbullah Drug and Money Laundering Scheme’, US Drug Enforcement Administration, 1 February 2016.

26. *Ibid.*

27. ‘Treasury Sanctions Key Hizbullah Money Laundering Network’, US Treasury Department, 28 January 2016.

28. *Ibid.*

prosecutors in Germany have opened at least 37 preliminary criminal investigations of persons tied to Hizbullah.²⁹

Businesses

While Dani Tarraf's company was based in Europe, in other cases Hizbullah established companies elsewhere for the purpose of procuring items from around the world, including Europe. Consider the July 2014 designation of brothers Kamel and Issam Amhaz and Ali Zeiter, who functioned as 'a key Hizbullah procurement network', according to the US Treasury Department. Using a Lebanon-based consumer electronics business, Stars Group Holding, as a front for a variety of illicit activities, the network allegedly purchased technology around the world – in North America, Europe, Dubai, and China – to develop drones for Hizbullah.³⁰

But Hizbullah also leverages businesses for massive financial profit as well. For example, in January 2016 the US Treasury designated Ali Youssef Charara and his company, Spectrum Investment Group Holding SAL, for supporting Hizbullah. Among other things, Spectrum Investment provides telecommunications in Europe.³¹ The US State Department reports that 'Charara has received millions of dollars from Hizbullah to invest in commercial projects that support the terrorist group'.³²

In May 2018, the US Treasury designated Hizbullah financier Mohammad Ibrahim Bazzi – a dual Belgian-Lebanese citizen who holds passports from Belgium, the UK, Lebanon, and Sierra Leone – as well as five companies he owns or controls. According to information released by the Treasury Department, Bazzi has provided millions of dollars to Hizbullah from the businesses he operates in Belgium, Lebanon, Iraq, and several West African countries.³³ One of the designated companies was Global Trading Group (GTG) NV, a Belgian energy services conglomerate. Bazzi is one of the founders and a Managing Director of GTG, which is headquartered

in Antwerp and has other locations in Sierra Leone, The Gambia, Ivory Coast, and Benin.³⁴ Bazzi is also tied to the Ayman Joumaa drug trafficking and money laundering organisation, Treasury noted. According to the State Department, Bazzi 'is a key Hizbullah financier, who has provided millions of dollars to Hizbullah generated from his business activities'.³⁵

Following his designation, Mohammad Bazzi tried to use his Belgium-based son, Wael Bazzi, as a cut-out to continue doing business. Wael and another Belgium-based GTG employee changed the company's name to Energy Engineers Procurement and Construction, listing Wael as the owner of the European company. In April 2019, the US Treasury designated Wael Bazzi, and another of his Belgium-based companies, Voltra Transcor Energy BVBA, as a measure to disrupt Hizbullah financing through the use of 'seemingly legitimate businesses'.³⁶

Abuse of Charity

Hizbullah has a long history of opening charities that function as fronts raising funds for the group, leading authorities around the world to investigate and shutter non-governmental organisations raising funds for the group. One of the latest examples is the Lebanon Orphan Children Project, based in Essen, Germany. In August 2014, German police raided several offices with ties to the Orphan Children Project and the Ministry of Interior outlawed the organisation and froze its funds. 'The name of this organisation masks its real purpose', Undersecretary for the Interior Emily Harber said at the time.³⁷

German authorities reported first investigating Orphan Welfare Project in 2009, likely after the revelation that the head of the organisation, Hisham Hassan, recruited an Israeli-Arab medical student studying in Germany for Hizbullah.³⁸ The student, Khaled Kashkoush, was introduced to a Hizbullah handler and tasked with collecting information on Israel and Israelis studying

29. 'Hezbollah's Links to Organized Crime in Germany', German Parliament 19th Legislative Period, Scientific Service of the Bundestag, 5 April 2019.

30. 'Treasury Sanctions Procurement Agents of Hezbollah Front Company Based in Lebanon with Subsidiaries in the UAE and China', US Treasury Department, 10 July 2014.

31. 'Treasury Sanctions Hizballah Financier and his Company', US Treasury Department, 7 January 2016.

32. 'Lebanese Hizballah's Financial Network', Rewards for Justice, US State Department.

33. 'Treasury Targets Key Hizballah Financing Network and Iranian Conduit', US Treasury Department, 17 May 2018.

34. *Ibid.*

35. 'Lebanese Hizballah's Financial Network', Rewards for Justice.

36. 'Treasury Targets Sanctions Evasion Conduits for Major Hizballah Financiers', US Treasury Department, 24 April 2019.

37. 'Germany Outlaws Support Group with Hezbollah Ties, Raids Offices Nationwide', *Deutsche Welle*, 4 August 2014.

38. *Ibid.*

abroad.³⁹ On appeal, Germany's Federal Administrative Court upheld the decision to ban the Orphan Children Project, noting that the group provided nearly €3.3 million to Hizbullah's Shahid (Martyr) Foundation, which the court described as 'an integral part of Hizbullah'.⁴⁰

In other cases, Hizbullah activists solicit private donations from Lebanese and Shia expatriate communities. For example, alongside its covert activities, Hizbullah's Foreign Relations Department (FRD) operates in a semi-public manner raising funds, recruiting supporters, providing logistical support, and collecting intelligence for Hizbullah. FRD personnel include both Hizbullah activists sent abroad from Lebanon and local Hizbullah supporters living abroad. Hizbullah's FRD has long been active in Europe. For example, Hizbullah sent FRD delegations to Denmark, Italy, Germany, Switzerland, and the UK in 2002–3 for the purpose of trying to keep the group off the EU terrorism list and bolster support and fundraising within local Lebanese and Shiite communities in Europe. The UK government has long acknowledged 'a small, overt Hizbullah presence in the UK with extensive links' to the FRD and, since the FRD reports to Hizbullah's political not terrorist leadership, tolerated its fundraising and other activities until the government's decision last year to expand its designation to include Hizbullah in its entirety.⁴¹

Conclusion

Hizbullah financing in Europe has not diminished since the EU's partial designation of the group in July 2013. While some of the cases discussed here predate the designation, many came afterwards. The designation empowered EU member states to do much more regarding Hizbullah terrorist operations, but less so when it comes

to the group's financial activities. Unless a given action is explicitly tied to Hizbullah's terrorist or military activities, it is not covered under the designation. And while the EU's Common Position 931 allows for designations of Hizbullah terrorist entities, it does not require them. In other words, such actions still require the political will to use this authority and such will has been in short supply. Beyond the question of a broader EU designation, however, European investigations into financial crime need to be more intelligence-driven to be able to target the types of activities carried out by illicit and covert organisations such as Hizbullah and its criminal associates. Operation Cedar stands out as a tremendous success, but it came about as a result of intelligence developed outside of Europe and shared with European partners. To make Europe a less hospitable jurisdiction for Hizbullah's criminal and other financing schemes European authorities will have to take the lead in developing cases. Until that happens, Hizbullah is likely to continue seeing Europe as a comfortable place to raise funds.

Matthew Levitt is the Fromer-Wexler fellow and director of the Reinhard program on counterterrorism and intelligence at The Washington Institute for Near East Policy. He sits on the advisory board for RUSI's Centre for Financial Crime and Security Studies, and is the author of *Hezbollah: The Global Footprint of Lebanon's Party of God*.

39. 'Arrest of Hezbollah Agent from Kalansua', Israel Ministry of Foreign Affairs, 6 August 2008.

40. German Federal Administrative Court in the contentious administrative matter of the Association Farber fur Waisenkinder e.V., 16 November 2015 (author's translation).

41. Matthew Levitt, 'Hezbollah's 'Diplomats' Go Operational', PolicyWatch 2734, The Washington Institute, 2 December 2016.



New Technologies but Old Methods in Terrorism Financing

Jessica Davis

About Project CRAFT

Project CRAFT 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 CRAFT is funded by the European Union'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 projectcraft.eu.

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

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



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

Terrorists are adaptive: they update their tactics and techniques by adopting new weapons systems, communication and surveillance technologies and organisational structures. They are also adaptive and innovative in the financial space, and exploit new technologies to raise, use, move, manage, store and obscure their funds. Terrorist groups, cells and individuals have all exploited technology with variation in scope and scale, but with remarkable similarity to existing financing methods. As the world has moved more of its day-to-day functions online and embraced things like online retailers and marketplaces, new financial technologies and cryptocurrency, as well as social media and crowdfunding platforms, terrorists have followed suit. Terrorists exploit these technologies to procure weapons and components, sell propaganda, move funds internationally and solicit donations from their supporters around the world. Countering the use of technology by terrorists to finance their activities involves ‘following the money’ to identify actors and operational activity, stopping funds whenever possible, and exploiting financial intelligence to illuminate terrorist intent, capability, planning and preparation.

Online Retailers and Marketplaces

Terrorists use online retailers and marketplaces like Amazon, eBay, Alibaba and other regionally specific platforms to procure goods and material for organisational needs as well as operational activity like terrorist attacks. Many also use these platforms to raise funds through the sale of propaganda and goods.

Terrorists use these platforms to obtain weapons and components for their attacks. For instance, the Islamic State bought drones and shipped them to Syria from a number of different online retailers.¹ Terrorists involved in the 2015–16 attacks in France and Belgium are believed to have bought weapons online from sources in the Balkans,² and in 2017, some of the material for the Manchester bombing was acquired online from Amazon.³

Terrorists likely purchase weapons and components online out of convenience, but also to reduce their interaction with members of the public, limiting the possibility that a bystander might observe suspicious activity and report it to the police.⁴

Online retailers and marketplaces also provide a venue for terrorists and extremists to sell goods and propaganda, raising small amounts of money while also spreading their message. Most of this activity is done to support individuals or cells rather than larger terrorist groups, and likely goes towards daily subsistence rather than directly for attack purposes. For instance, Atomwaffen Division (a neo-Nazi extremist group based in the US) members raised funds by selling books, specifically *Siege*, a collection of essays by US neo-Nazi James Mason and a critical piece of Atomwaffen’s ideological apparatus, on Amazon’s CreateSpace.⁵ Propaganda sales are unlikely to generate significant profit for terrorists and extremists, but generate a small source of funds, create loose networks of likeminded individuals and serve to keep propaganda available to potential new recruits.

Online retailers and marketplaces have also been used by terrorist groups (or their proxies) to sell looted goods. For instance, antiquities looted from Islamic State territory were found for sale on eBay and in Facebook groups and community pages,⁶ while antiquities traffickers have also made deals using Skype, WhatsApp or Kik messaging services.⁷ The Islamic State profited from the sale of antiquities by taxing it at source and by looting artefacts and selling them to intermediaries, even though they were unlikely to have conducted the online sale of the goods directly.

Cryptocurrencies and Financial Technologies

Financial technologies enable terrorists to transfer funds between people, facilitate payments and move money around the world instantaneously. Terrorists and

1. Don Rassler, ‘The Islamic State and Drones: Supply, Scale, and Future Threats’, Combating Terrorism Center at West Point, 11 July 2018.
2. Mitch Prothero, ‘Inside The World Of ISIS Investigations In Europe’, *BuzzFeed News*, 21 August 2016.
3. BT, ‘Manchester Arena Accused Foiled in Bid to Obtain “Bomb Ingredient”, Court Told’, 5 February 2020, <<http://home.bt.com/news/latest-news/manchester-arena-accused-foiled-in-bid-to-obtain-bomb-ingredient-court-told-11364429917547>>, accessed 10 February 2020.
4. Counter Terrorism Policing, ‘Episode One: Multiple Bombings’, Code Severe Podcast Series, <<https://www.counterterrorism.police.uk/code-severe-podcast/>>, accessed 10 February 2020.
5. Alexander Epp and Roman Höfner, ‘The Hate Network: Atomwaffen Division’, *Der Spiegel*, 7 September 2018.
6. Steve Swann, ‘Antiquities Looted in Syria and Iraq are Sold on Facebook’, *BBC News*, 2 May 2019.
7. Rachel Shabi, ‘Looted in Syria – and Sold in London: The British Antiques Shops Dealing in Artefacts Smuggled by Isis’, *The Guardian*, 3 July 2015.

extremists solicit donations from their supporters and encourage them to use financial technologies, often touting the anonymity or increased privacy of these tools over that of banks or traditional money service businesses.

The most popular cryptocurrency among terrorists and extremists is by far Bitcoin, lauded for its supposed anonymity as well as the mythology surrounding its creation.⁸ Terrorists and extremists have used Bitcoin to move money and to pay for services like as webhosting,⁹ although terrorists (particularly the Islamic State) also use other cryptocurrencies like Monero.¹⁰ The most common terrorist use of cryptocurrency is to solicit donations from supporters. A number of terrorist organisations have solicited donations in Bitcoin, but Hamas's foray into the cryptocurrency space has been particularly interesting.¹¹ Initially, Hamas publicly posted its wallet address on the donation website, which made all the donations to it traceable. Over time, Hamas has improved its financial tradecraft, and now generates a new wallet for every donation, significantly enhancing its operational security and making it far more difficult to 'follow the money'.¹²

Individual terrorist supporters have also used cryptocurrency to move funds to terrorist groups. In December 2017, Zoobia Shahnaz was arrested for raising over \$85,000 to send to the Islamic State.¹³ She used false information to acquire loans and multiple credit cards in order to raise the funds, then purchased Bitcoin and other digital currencies and sent them to the terrorist group.¹⁴ At the same time, while terrorists have used Bitcoin and other cryptocurrency to move funds, evidence of direct operational funding through Bitcoin and other cryptocurrency has, to date, largely been exaggerated.¹⁵

The use of financial technology by terrorists and extremists is not restricted by ideology, and it appeals to

individuals across the political spectrum. For instance, some far-right figures have websites where they accept individual donations through credit card companies or PayPal and publicly identify their Bitcoin wallet. They also use crowdfunding sites like Patreon to generate financial support. For instance, Canadian white nationalist Faith Goldy has been financially deplatformed by a number of financial technology companies,¹⁶ but maintains a Bitcoin address and accepts credit card payments via her website.¹⁷

Bitcoin, and to a lesser extent other financial technologies, appeal to these actors in part because they are perceived to avoid the financial surveillance of the formal financial sector. At the same time, the pseudo-anonymous nature of transactions can be combined with other forms of financial tradecraft to increase anonymity and obscure the source and destination of funds. Many of the people who donate to terrorist and extremist groups employ basic financial tradecraft and operational security measures such as the use of Bitcoin exchanges or tumblers, the use of new wallets to minimise the number of transactions that can be directly linked to them, or a combination of techniques. As some cryptocurrency researchers have noted, Hamas's adoption of some of these techniques (such as new wallets for every Bitcoin transaction) has greatly increased the difficulty in tracking transactions.¹⁸

Cryptocurrencies will not replace traditional financing methods for terrorists. Cash couriers, hawalas, the banking sector and other methods of moving money will remain integral to the financial tradecraft of terrorists. However, cryptocurrencies and other financial technologies will be adopted when practical and when they provide an additional layer of obfuscation for the source and destination of funds.

8. Nathaniel Whittemore, 'The Shadow of Satoshi's Ghost: Why Bitcoin Mythology Matters', *CoinDesk*, 22 May 2020, <<https://www.coindesk.com/the-shadow-of-satoshis-ghost-why-bitcoin-mythology-matters>>, accessed 10 February 2020.
9. Financial Action Task Force, 'Financing of Recruitment for Terrorist Purposes', January 2018, <<http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-Recruitment-for-Terrorism.pdf>>, accessed 1 December 2018.
10. Andrey Shevchenko, 'ISIS-Affiliated News Website to Collect Donations with Monero', *Cointelegraph*, 25 June 2020, <<https://cointelegraph.com/news/isis-affiliated-news-website-to-collect-donations-with-monero>>, accessed 1 July 2020.
11. Michael Arnold and Saud Abu Ramadan, 'Hamas Calls on Supporters to Donate to Group in Bitcoin', *Bloomberg*, 30 January 2019.
12. Popular Front, 'Bonus: Tracking the Hamas Bitcoin Wallet', <<https://podcasts.apple.com/gb/podcast/bonus-tracking-the-hamas-bitcoin-wallet/id1364539980?i=1000475847072>>, accessed 1 July 2020.
13. Leigh Cue, 'New York Woman Charged With Laundering Bitcoin for ISIS', *International Business Times*, 15 December 2017, <<http://www.ibtimes.com/new-york-woman-charged-laundering-bitcoin-isis-2629112>>, accessed 1 July 2020.
14. Harriet Alexander, 'New York Woman Charged with Sending \$85,000 in Bitcoin to Support Isis', *The Telegraph*, 14 December 2017.
15. Jessica Davis, 'A Canadian Cryptocurrency Caper in the Sri Lanka Attack? Unlikely', *INTREPID*, 6 May 2019, <<https://www.intrepidpodcast.com/blog/2019/5/6/a-canadian-cryptocurrency-caper-in-the-sri-lanka-attack-unlikely>>, accessed 6 May 2019.
16. Canadian Anti-Hate Network, 'Faith Goldy', <https://www.antihate.ca/tags/faith_goldy>, accessed 2 July 2020.
17. Personal website of Faith Goldy, <<https://faithgoldy.ca/donations/>>, accessed 9 July 2020.
18. Popular Front, 'Bonus: Tracking the Hamas Bitcoin Wallet'.

Social Media and Crowdfunding

Terrorists and extremists across the political spectrum have exploited social media and crowdfunding platforms to raise funds. They have used social media platforms to solicit funds from donors and crowdfunding platforms to raise funds, often under the guise of charitable activity. When terrorists use social media for their funding calls, they often redirect supporters to other payment mechanisms. More recently, the incorporation of native payment systems in social media platforms has enabled terrorists to move funds within the platform. Terrorists also use messaging platforms like WhatsApp, Kik and others to arrange for the sale of goods and transfer of funds.

While soliciting funds from support networks is an old terrorist financing method, social media makes it easier for terrorist actors to reach and receive donations from a wider audience. For instance, Hajjaj Fahd Al Ajmi, a Kuwait national who served as a focal point for donations to Al Nusrah Front, had a robust and active presence on Instagram and Twitter, and he used these platforms to solicit funds from supporters.¹⁹ Al Shabaab has also used social media to solicit funds from its support network outside of Somalia. In 2016, two women led a support network of 15 women in fundraising for Al Shabaab. The women solicited money in a chat room, and sent that money (likely through a hawala or money service business) to financiers of Al Shabaab where the money was used to finance military operations in Somalia. The group of women included supporters from Somalia, Kenya, Egypt, the Netherlands, Sweden, the UK, Canada and Minneapolis.²⁰

Support networks can also be mobilised to provide financial assistance to detained terrorists. For instance, suspected Islamic State members in Syria (women detained in camps for Islamic State families) have raised thousands

of dollars through online crowdfunding campaigns. Two such campaigns explicitly aimed to raise funds to pay smugglers to help them escape from their detention camps. Many of these crowdfunding activities also cross platforms, starting as a call on one (such as Instagram) before redirecting the potential donor to a payment platform like PayPal.²¹

Terrorist attacks have also been funded through crowdfunding, although examples of this are rare. This fundraising technique may be used specifically in cases where terrorists do not have enough money on hand for their desired operational activities and seek out avenues to acquire funds. This includes applying for and receiving a loan just days before an attack, as the perpetrators of the San Bernardino attack did in 2015.²² The loan was provided by Prosper Marketplace, a financial technology and crowdfunding company that provides peer-to-peer lending, amounting to \$28,500.²³ The perpetrators used some of these funds to provide for their child after their attack, using the rest to purchase components for the 12 pipe bombs found at their residence and the over 4,500 rounds of ammunition, in addition to the ammunition used during the attack.²⁴

While recent terrorist financing schemes using crowdfunding websites have drawn significant attention, this is not a new technique. Terrorists have solicited funds from their supporters for decades.²⁵ What is new is the use of financial technology, and specifically social media and crowdfunding websites to facilitate it. The premise employed in the past is the same as today – websites, often crowdfunding sites, advertise the purchase of goods, weapons, or supplies for terrorists (or using a cover story), and donors can provide the funds. But today, transactions can occur instantaneously and can be made more anonymous by combining social media, financial technologies and cryptocurrencies.

19. UN Security Council, 'Hajjaj Bin Fahd Al Ajmi', <https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/individual/hajjaj-bin-fahd-al-ajmi>, accessed 2 July 2020.
20. Dan Whitcomb, 'Two Women Convicted in U.S. of Financing Somali Group Al Shabaab', *Reuters*, 25 October 2016.
21. Audrey Alexander, "'Help for Sisters": A Look at Crowdfunding Campaigns with Potential Links to Terrorist and Criminal Networks', Global Network on Extremism & Technology (GNET), 11 June 2020, <<https://gnet-research.org/2020/06/11/help-for-sisters-a-look-at-crowdfunding-campaigns-with-potential-links-to-terrorist-and-criminal-networks/>>, accessed 2 July 2020.
22. Comply Advantage, 'Money in Terrorist Hands: What FinTech Firms Should Fear', 14 December 2015, <<https://complyadvantage.com/blog/money-in-terrorist-hands-what-fintech-firms-should-fear/>>, accessed 2 July 2020.
23. Maggie McGrath, 'Why It Would Have Been Perfectly Legal for the San Bernardino Shooter to Borrow \$28,400 From Prosper', *Forbes*, 8 December 2015.
24. *BBC News*, 'San Bernardino Shooting: Who Were the Attackers?', 11 December 2015.
25. Barry A K Rider, 'The Weapons of War: The Use of Anti-Money Laundering Laws Against Terrorist and Criminal Enterprises—Part 1', *Journal of International Banking Regulations* (Vol. 4, No. 1, 2002), p. 18.

Counterterrorism Financing Implications

As financial technologies evolve, so will terrorist financing techniques that exploit them, meaning that countering this activity effectively will require ongoing adaptation to new technologies and platforms.

Countering terrorist financing through online retailers or marketplaces requires addressing how terrorists use these platforms: to acquire weapons and components, as well as fundraising through the sale of propaganda and goods. Online retailers and marketplaces are well placed to track and monitor online sales, including specific combinations of goods. However, even basic efforts by the prospective terrorist to hide the purpose or destination of the goods may complicate these efforts, and this activity is easily displaced from one platform to another. Using online retailers and marketplaces allows terrorists to procure goods and avoid suspicion that might arise from interacting with staff in person, reducing opportunities for law enforcement and security services to detect plots.²⁶ From a counterterrorist financing perspective, it may prove more beneficial for these companies to report concerning or suspicious activity to law enforcement rather than simply prohibit it, as this information can provide investigative leads. Educating companies about how their technologies are being used to facilitate terrorist financing is a first step; regulation and mandatory reporting may be required or warranted as well. Similarly, while it may be tempting to force companies to take down propaganda or goods being sold by terrorists or extremists, these sales can provide valuable financial intelligence to investigators, although encouraging companies to continue to allow these activities to take place may require the adoption of 'keep open' orders for online retailers or marketplaces.²⁷

Financial technologies and cryptocurrencies appeal to terrorists as a means of safely and securely moving money from supporters and for operational needs. At the same time, many of these technologies have anti-money laundering or counterterrorist financing reporting requirements, meaning that they are not necessarily anonymous or secret, even if they do have other benefits such as price and speed.

For terrorists and extremists, some of these technologies also have barriers to entry making them difficult to use, all of which reduces their widescale adoption. However, the preponderance of technologies that can be used to move money complicates investigations – understanding and exploiting these technologies for leads requires ongoing situational awareness of dozens, if not hundreds, of applications and tools. Few law enforcement services in the world have the personnel to do this effectively. Tools and guidance developed by international organisations such as the FATF, the Egmont Group or the UN Office on Drugs and Crime would help states exploit financial technologies for financial intelligence and facilitate greater investigative capacity in this space, reducing the burden on counterterrorism forces to become experts in everything new and novel, and allowing them to focus on the important part of the transaction – the sender and beneficiary.

Social media platforms, and to a lesser extent crowdfunding platforms, are no strangers to the controversies surrounding terrorist use of their platforms. Many are already well equipped with internal policies to 'take down' extremist materials, including calls for funds. However, many of these policies are poorly or inconsistently enforced, and in some cases, social media companies or messaging services have little or no interest or incentives to remove extremist content. In the case of terrorist financing, take downs may be attractive solutions for the perceived inherent public good of removing extremist content,²⁸ but this strategy should be balanced with the need to develop and acquire financial intelligence for investigations. There is no simple equation to achieve this balance – an ongoing dialogue and partnership between counterterrorism practitioners and these platforms is required to achieve the right balance, and decisions will need to be taken on a case-by-case basis.

The use of technology by terrorists and extremists for financing is by no means new nor are the underlying methods, but the specific technologies and techniques they use will continue to evolve with changes in technology and financial systems. The adoption of these technologies does not represent a paradigm shift in terrorist financing, but it does complicate investigations, challenge legislation and regulation of these platforms, and necessitate

-
26. Jessica Davis, 'How Terrorists Use the Internet for Weapons and Component Procurement', GNET, 26 February 2020, <<https://gnet-research.org/2020/02/26/how-terrorists-use-the-internet-for-weapons-and-component-procurement/>>, accessed 26 February 2020.
27. Nick J Maxwell, 'Expanding the Capability of Financial Information-Sharing Partnerships', *RUSI Occasional Papers* (March 2019).
28. Tom Keatinge and Florence Keen, 'Social Media and Terrorist Financing: What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better?', *Global Research Network on Terrorism and Technology Paper*, 2 August 2019.

enhanced public–private partnerships.²⁹ To effectively counter terrorist financing through new technologies, acknowledgement of the significant differences between how terrorist organisations finance their activities and how operational cells and individuals do so is critical. It is also increasingly important to understand the difference between terrorist organisations and extremist movements, the latter of which are unlikely to have a centralised financing structure, but where members use a wide variety of technologies to raise, use, move and obscure their funds. It is also critical to balance actions meant to prevent terrorists from acquiring funds, goods and material with the financial intelligence that can be gleaned from these transactions. Ultimately, counterterrorist financing needs to focus on stopping the money wherever possible, while balancing that with following and exploiting financial intelligence and using that intelligence to illuminate terrorist intent, capability, planning and preparation.

Jessica Davis is a former senior strategic analyst with the Canadian Security Intelligence Service and is the president and principal consultant at Insight Threat Intelligence, a global security consulting firm. She is the author of *Women in Modern Terrorism: From Liberations Wars to Global Jihad and the Islamic State* (Lanham, MD: Rowman & Littlefield, 2017).

29. Patrick Hardouin, 'Banks Governance and Public–Private Partnership in Preventing and Confronting Organized Crime, Corruption and Terrorism Financing', *Journal of Financial Crime* (Vol. 16, No. 3, July 2009), pp. 199–209.



Financial Intelligence in the Age of Lone Actor Terrorism

Stephen Reimer and Matthew Redhead

About Project CRAFT

Project CRAFT 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 CRAFT is funded by the European Union'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 projectcraft.eu.

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

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



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

Europol, the EU's policing agency, assesses that 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'.¹ According to its latest annual Terrorism Situation and Trend Report, this threat comes from both Islamist extremism and, increasingly, the far-right.² Despite the coronavirus pandemic, the threat remains immediate and ongoing and lone actor attacks continue across Europe, undeterred by social restrictions. In April 2020, two were killed and five wounded in a knife attack in Romans-sur-Isère, France; in June, three were killed and three injured in a stabbing in Reading.

Such lone actor and small cell (LASC) attacks have created an acute challenge for counterterrorism (CT) efforts, which, for the first 15 years of this century, had largely benefited from terrorists undertaking controlled, coordinated attacks which were more easily detectable.³ This challenge is felt acutely by CT's financial arm, the counterterrorist finance (CTF) regime, which, built on the presumption that terrorist networks use the formal financial system to fund spectacular attacks, now seems largely redundant in the face of undetectable simplicity.

CTF is struggling therefore, in the age of LASCs. Financial intelligence (FININT) – information on a target's financial affairs – might be put to better use if deployed to enrich CT intelligence and large-scale surveillance, prioritising the apparently lower-order targets who, increasingly, have gone on to become lone actors. To deliver this change, however, the CTF regime will need to be reconfigured around stronger, more direct partnerships between financial institutions (FIs) and intelligence, security and law enforcement agencies than have existed up to now.

Scope and Caveats

This research briefing is the third deliverable of five in the RUSI Europe project 'Lone Actor and Small Cell Terrorism and the Future of CTF', which reviews the recent evolution of the terrorist threat in Europe across all ideological backgrounds, and considers the implications for the future of CTF. The briefing was preceded by a literature review and a digest of research interviews,⁴ and will be followed by a collection of case studies of recent LASC attacks focusing on France, Germany, Sweden and the UK, and a final report, due in early 2021. This year-long project is part of a three-year multi-partner research programme on CTF, 'Project CRAFT', funded by the European Commission.⁵

Defining LASCs

The academic literature around the term 'lone actors and small cells' is inconclusive and definitions remains disputed;⁶ this briefing therefore sidesteps that debate for the time being, using a working definition that follows Europol in prioritising the importance of *operational autonomy* as the mark of a LASC. LASCs choose to undertake an attack and prepare and execute it themselves, but they are not necessarily unconnected to wider extremist networks.⁷ Of course, the existence of actors' wider links to other extremists creates 'boundary' cases, where operational autonomy might be difficult to perceive. However, this is in the nature of the area of study; determining the level of personal sovereignty over an attack can be difficult to unpick, and such assessments have to be made on a case-by-case basis.

1. Europol, 'European Union Terrorism Situation and Trend Report (TE-SAT) 2020', 23 June 2020, <<https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020>>, accessed 6 August 2020, p. 19.
2. *Ibid.*
3. For example, consider the 2006 Al-Qa'ida-linked transatlantic liquid bomb plot that was foiled by UK law enforcement. See Dominic Casciani, 'Liquid Bomb Plot: What Happened', *BBC*, 7 September 2009.
4. Both previous deliverables are working documents not for publication.
5. Collaboration, Research and Analysis Against the Financing of Terrorism (Project CRAFT), <<https://www.projectcraft.eu>>.
6. Michael Fredholm (ed.), *Understanding Lone Actor Terrorism: Past Experience, Future Outlook, and Response Strategies* (London: Routledge, 2017), pp. 1–28.
7. See also Paul Gill, John Horgan and Paige Deckert, 'Bombing Alone: Tracing the Motivations and Antecedent Behaviours of Lone-Actor Terrorists', *Journal of Forensic Sciences* (Vol. 59, No. 2, 2014), pp. 425–35.

The Origins of the Threat

The emergence of the Islamist LASC threat in Europe is rooted largely in operational necessity. Between Al-Qa'ida's (AQ) 9/11 attacks and the precipitous decline of the Islamic State's territorial empire from 2016 onward, Europe faced a cell-based Islamist extremist threat, largely directed from overseas. Such 'networked' cells mounted ambitious and highly lethal attacks, using improvised explosive devices (IEDs)⁸ and, later, coordinated armed attacks.⁹ However, increased surveillance and international governmental cooperation proved extremely effective in degrading these capabilities and the command structures behind them.¹⁰ As a consequence, these much reduced networks have gone digital, using social media and online messaging to radicalise and motivate individuals to undertake their own attacks in the name of the movement.¹¹

The far-right terrorist threat, which has developed more recently, has emerged into the same operational realities, and is likely to have been shaped by it in similar ways. However, it is possible that their adoption of a 'lone actor' approach is also shaped by conscious copying of Islamist extremist tactics, as well as a preference for the emulation of 'heroic' loners such as Brenton Tarrant, who attacked mosques in Christchurch in March 2019.¹² Indeed, Philip Manshaus, who attacked an Islamic centre in an Oslo suburb in August 2019, was directly inspired by Tarrant, who he idolised, having posted online on the day of his attack: 'My time is up, I was chosen by Saint Tarrant after all'.¹³

The Attackers

There is no detailed 'profile' for a lone actor or small cell.¹⁴ Among recent Islamist extremists researched for the project so far, most come from modest socioeconomic backgrounds, living off low-income jobs, benefits and student loans. In France, Mohamed Lahouaiej-Bouhlel, the Nice truck attacker of July 2016, was a delivery driver, while Mohamed Hichem Medjoub, suspected of the Lyon letter bombing of May 2019, was dependent on online teaching.¹⁵ Several others have exhibited links to petty criminality.¹⁶ Far-right LASCs also appear to be from relatively deprived socioeconomic backgrounds, and with even greater tendencies towards unusual levels of social isolation. Thomas Mair, who assassinated British MP, Jo Cox, in June 2016, and Tobias Rathjen, the Hanau shisha bar attacker of February 2020, both lived solitary lives and are reported to have had mental health problems.¹⁷

The Attacks

LASC attacks can be ambitious, such as the truck bomb and firearms assaults in Oslo and Utøya by Anders Breivik in July 2011.¹⁸ However, such attacks can leave a large operational footprint, making them vulnerable to detection, and require substantial technical expertise and autonomy to pull-off successfully. Extremists now operate in an environment where any plot-relevant ties may expose them to intelligence agencies. The vast majority of would-be attackers also lack the technical skills, competence and stealth of the likes of Breivik. It is little surprise therefore that LASCs have become increasingly likely to carry out basic attacks completely on their own, using easily sourced domestic weapons such as vehicles and knives. Indeed, in the last year, knives have increasingly predominated among Islamist extremists, used for

8. For example, the 2004 Madrid train bombings.

9. For example, the 2015 attacks on the Paris offices of *Charlie Hebdo*.

10. Videoconference interview with former UK intelligence officer, 20 May 2020.

11. Videoconference interview with Peter Neumann, International Centre for the Study of Radicalisation and Political Violence (ICSR), Kings College London (KCL), 4 May 2020.

12. Videoconference interview with Florence Keen, ICSR, KCL, 1 May 2020.

13. Jason Burke, 'Norway Mosque Attack Suspect "Inspired by Christchurch and El Paso Shootings"', *The Guardian*, 11 August 2019.

14. Paul Gill, *Lone Actor Terrorists: A Behavioural Analysis* (London: Routledge, 2016), p. 26.

15. Videoconference interview with French law enforcement official, 9 July 2020.

16. Videoconference interview with Peter Neumann.

17. *BBC News*, 'Thomas Mair: Extremist Loner Who Targeted Jo Cox', 23 November 2016; *New Straits Times*, 'The Bizarre Views of Germany Shooter Tobias Rathjen', 22 February 2020, <<https://www.nst.com.my/world/world/2020/02/567892/bizarre-views-germany-shooter-tobias-rathjen>>, accessed 23 August 2020.

18. Bart Schuurman et al., 'End of the Lone Wolf: The Typology That Should Not Have Been', *Studies in Conflict and Terrorism* (Vol. 42, No. 8, 2019), pp. 771–78.

example in the Paris police headquarters attack in October 2019, the London Bridge attack of November 2019, and the Romans-sur-Isère and Reading attacks of 2020.

Far-right LASCs have also used similar means. For example, white supremacist Vincent Fuller used a knife in an attack on immigrants in Stanwell, in the UK, in September 2019. However, far-right LASC attacks also feature firearms assaults, such as those seen in Halle and Hanau in Germany, in October 2019 and February 2020 respectively. These attacks again demonstrate the appeal within the far-right of imitating the styles of attack used by movement ‘heroes’ such as Breivik and Tarrant.¹⁹

The CTF Challenge

The current LASC threat – self-contained, furtive and low-profile – thus poses major investigative challenges for the authorities. More basic attacks are more difficult to detect, and their perpetrators, even if previously ‘on the radar’, tend to be peripheral figures in extremist ecosystems. If LASCs are a challenge to CT, however, they are an even greater problem for CTF. The CTF regime that emerged after 9/11 is built on a ‘corporate’ vision of terrorist finances, typical of formal groups such as Hizbullah or Hamas. Under the regime, terrorists are to be ‘starved’ of funds by pre-existing anti-money laundering tools, comprised in the Financial Action Task Force’s 40 recommendations.²⁰ FIs act as ‘gatekeepers’ of the financial system, screening customers against watchlists, freezing accounts, and reporting concerning activity to the authorities via Suspicious Activity or Suspicious Transaction Reports (SARs or STRs).²¹

Even before the rise of LASCs, the adequacy of this approach had been under scrutiny for some time.²² Only a few years after 9/11, ‘networked’ attacks were being largely self-funded without any international support. For example, the AQ-linked cell that attacked the London transport network on 7 July 2005 deployed four homemade IEDs, at the cost of just £8,000, which the cell was able to fund through their own wages and a loan.²³ According to one former law enforcement interviewee, the current style of LASC attacks makes this problem tougher still, because the financial signals from a simple attack are meagre, and the controls FIs have in place to detect them are not sophisticated enough to filter out an inoperably high rate of false positives.²⁴

Assessing the Challenge

FI CTF controls, especially transaction monitoring platforms, are certainly inadequate to the task of detecting LASC behaviours. No more than 14% of alerts – at best – are deemed sufficiently convincing to result in a SAR,²⁵ and only 1–2% of these SARs go on to form the basis of an investigation.²⁶ Trying to identify potential LASCs with tools such as these is like trying to catch a gnat in a butterfly net.

FININT itself, however, is not necessarily without utility. Some LASCs are so marginal as to produce no financial information of interest to CT authorities at all. Rakhmat Akilov, an Islamist extremist who mounted a truck attack in Stockholm in April 2017, had no significant financial profile, and stole the vehicle he used.²⁷ But ongoing case studies for this project suggest that LASCs can produce an ‘exhaust trail’ of financial data that could, in combination with other intelligence, aid agencies’ understanding of their

19. Videoconference interview with Florence Keen.
20. Following 9/11, the Financial Action Task Force produced eight Special Recommendations on Terrorism Financing, which was increased to nine before these were mainstreamed into the revised 40 recommendations on anti-money laundering and counterterrorism financing in 2012.
21. Nicholas Ryder, *The Financial War on Terrorism: A Review of Counter-Terrorist Financing Strategies Since 2001* (London: Routledge, 2017), pp. 1–19.
22. Peter Neumann, ‘Don’t Follow the Money: The Problem with the War on Terrorist Financing’, *Foreign Affairs* (Vol. 96, No. 4, 2017), pp. 93–102.
23. House of Commons, *Report of the Official Account of the Bombings in London on 7th July 2005*, HC 1087, (London: The Stationery Office, 2006), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228837/1087.pdf>, accessed 7 August 2020, p. 23.
24. Videoconference interview with former UK law enforcement official, 4 June 2020.
25. EY, ‘Anti-Money Laundering (AML) Transaction Monitoring: 2018 EMEIA Survey Report’, October 2018, <<https://assets.ey.com/content/dam/>>, accessed 23 August 2020, p. 5.
26. Matthew Redhead, ‘Deep Impact? Refocusing the Anti-Money Laundering Model on Evidence and Outcomes’, *RUSI Occasional Papers* (October 2019), p. 16.
27. Videoconference interview with Magnus Ranstorp, Swedish National Defence College, and Swedish law enforcement official, 11 August 2020.

behaviours. In the run up to the Nice attack, for example, Lahouaiej-Bouhlel made significant cash withdrawals over a two week period that were not consistent with past behaviour; these funds subsequently went towards the cash purchase of a vehicle and a weapon for the attack.²⁸ From the vantage point of financial data alone, such behaviour would almost certainly be overlooked by the transaction monitoring systems used by FIs today. But this insight, especially about someone known but ‘low priority’, when combined with additional intelligence, could prove invaluable in both expanding the agencies’ view of the target’s network, as well as the relative threat they might pose.

FININT, Not CTF

Given that there can be tens of thousands of individuals of concern for the authorities at any one time,²⁹ the potential for more timely and targeted delivery of FININT by FIs, and its use by agencies, thus needs further exploration. Part of the answer is likely to come from applying the principles of pre-existing Financial Intelligence Sharing Partnerships between FIs and relevant agencies, such as the Joint Money Laundering Intelligence Task Force in the UK, more firmly to CT. However, most partnerships are currently managed through convened meetings, rather than permanent co-location or joint-working,³⁰ and although such existing arrangements are valuable, there are potentially more impactful ways in which the concept of CT ‘partnership’ might evolve outside the current CTF regime.

In several European jurisdictions, non-SAR ‘intelligence channels’ between FIs, intelligence and law enforcement agencies already exist, most of which predate 9/11.³¹ These usually travel in one direction – first, with FIs supplying material post-attack, and second, providing FININT under warrant for priority targets before any attack. However, such channels might be widened and exploited to cooperatively review and monitor a third

group of ‘lower priority cases’ from which LASCs often spring. Again, there are already some precedents for an institutionalised approach along these lines. In the UK, for instance, the authorities’ strategy to tackle LASCs has involved the creation of local ‘Multi-Agency Centres’, where the police and intelligence agencies work with health, education and welfare departments, mutually sharing information about ‘lower priority’ individuals in a secure and vetted environment.³² Initiatives such as this would almost certainly benefit from direct and permanent involvement from FIs.

Conclusion

As noted at the outset, this research briefing does not constitute the final word on the findings of the project. There will undoubtedly be variations between initial judgements here and those in the final paper. However, what is already apparent is that the ‘LASC threat’ has further exposed the underlying fissures in the global CTF architecture, which are unlikely to be rectified without a substantial change of perspective. FININT is not a panacea for the problems of LASCs, but it might – if properly deployed – play a more effective role in tackling the problem than it has so far. To make best use of FININT, European countries need more agile, fluid and timely intelligence channels between FIs and CT-focused agencies. The current CTF regime is not sufficient to help deal with the LASC threat, and it is therefore time to rethink it.

Stephen Reimer is a Research Analyst at the Centre for Financial Crime and Security Studies at RUSI.

Matthew Redhead is an Associate Fellow at the Centre for Financial Crime and Security Studies at RUSI.

28. Videoconference interview with French law enforcement official, 9 July 2020.

29. Dominic Casciani, ‘The Day I Tried to Be an MI5 Spook’, *BBC News*, 2 July 2019.

30. Nick Maxwell, ‘Survey Report: Five Years of Growth in Public–Private Financial Information-Sharing Partnerships to Tackle Crime’, *Future of Financial Intelligence Sharing (FFIS)*, RUSI, August 2020, p. 14.

31. Videoconference interview with former UK intelligence officer, 20 May 2020.

32. UK Home Office, *CONTEST: The United Kingdom’s Strategy for Countering Terrorism* (London: The Stationery Office, June 2018), p. 42.



Fraud-Enabled Terrorism Financing: A Neglected Dossier

Nicholas Ryder

About Project CRAFT

Project CRAFT 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 CRAFT is funded by the European Union'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 <projectcraft.eu>.

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

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



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <<http://creativecommons.org/licenses/by-nc-nd/4.0/>>.

Introduction

Terrorists are able to obtain finances from a wide range of sources as illustrated by those used by the Irish Republican Army (IRA), Al-Qa'ida, Hamas, Hizbullah, Boko Haram, Al-Shabaab and the Islamic State.¹ It was not until 9/11 that the international community instigated the 'Financial War on Terrorism', which was based on a series of counterterrorist financing legislative measures from the UN, EU and the Recommendations from the Financial Action Task Force (FATF).² The Financial War on Terrorism consists of five mechanisms: criminalisation; confiscation or forfeiture; asset freezing; a designated terrorism sanctions regime; and the use of suspicious activity reports. These mechanisms, especially the sanctions regime, have been able to limit the funding avenues of some terrorist groups, such as Al-Qa'ida.³ Therefore, as terrorists have been increasingly unable to secure enough funding via their traditional methods, they have had to turn towards other alternative sources, such as fraud. The legislative provisions have forced terrorism financiers to adapt their funding mechanisms and move away from their traditional funding sources.⁴ This paper presents evidence that terrorism financiers have used fraud to obtain funding, often without detection, and it

identifies a new and updated terrorism financing fraud typology.

Typologies have been used by the FATF and the IMF to identify the funding requirements of terrorist organisations.⁵ Typologies have focused on identifying the different types of fraudulent activity.⁶ Similarly, the Financial Conduct Authority, the National Fraud Authority, the Home Office and commentators have focused on identifying typologies of the victims of fraud.⁷ Despite their merit, the typologies have failed to identify the link between terrorism financing and fraud. For instance, the Home Office typology acknowledges that fraud is associated with other types of crime, but does not refer to terrorism. Conversely, there are a small number of typologies which have focused on terrorism financing and fraud.⁸ This research adds to the existing literature by highlighting how terrorism financiers have been able to accrue funding by different types of fraud, which this paper identifies as a terrorism financing fraud typology.

1. For general information, see HM Government, *Economic Crime Plan 2019–22* (London: The Stationery Office, 2019). For Al-Qa'ida, see Juan Miguel del Cid Gómez, 'A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates', *Perspectives on Terrorism* (Vol. 4, No. 4, 2010), pp. 1–25; Jimmy Gurule, *Unfunding Terror: The Legal Response to the Financing of Global Terrorism* (Cheltenham: Edward Elgar, 2008), chapters 2 and 3. For Hamas, see Counter Extremism Project, 'Hamas', <<https://www.counterextremism.com/threat/hamas>>, accessed 8 June 2020. For Hizbullah, Boko Haram and Al-Shabaab, see Financial Action Task Force (FATF), 'Terrorist Financing in West and Central Africa', October 2016; FATF, 'Emerging Terrorist Financing Risks', October 2015. For the Islamic State, see FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant', February 2015.
2. See Nicholas Ryder, *The Financial War on Terrorism: A Review of the Counter-Terrorist Financing Strategies Since 2001* (London: Routledge, 2015).
3. See Christopher Michaelsen, 'The Security Council's Al Qaeda and Taliban Sanctions Regime: "Essential Tool" or Increasing Liability for the UN's Counterterrorism Efforts?', *Studies in Conflict and Terrorism* (Vol. 33, No. 5), pp. 448–63 and J Gurule, J. *Unfunding Terror - The Legal Response to the Financing of Terror* (Cheltenham: Edward Elgar, 2008).
4. See Nicholas Ryder, 'A False Sense of Security? An Analysis of Legislative Approaches Towards the Prevention of Terrorism Finance in the United States and the United Kingdom', *Journal of Business Law* (2007), pp. 821–50; Umut Turksen and Nicholas Ryder, 'Banks in Defense of the Homeland: Nexus of Ethics and Suspicious Activity Reporting', *Contemporary Issues in Law* (Vol. 12, No. 4, 2014), pp. 311–47.
5. See FATF, 'Terrorist Financing', 29 February 2008; IMF, 'Anti-Money Laundering/Combating the Financing of Terrorism – Topics', <<https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm>>, accessed 1 January 2020.
6. See, for example, KPMG, 'Global Banking Fraud Survey', May 2019, p. 6.
7. Shannon Harvey et al., 'Understanding Victims of Financial Crime: A Qualitative Study with People Affected by Investment Fraud', NatCen, 3 March 2014, pp. 36–45; National Fraud Authority, 'Fraud Typologies and Victims of Fraud: Literature Review', 2009; Home Office, *The Scale and Nature of Fraud: A Review of the Evidence* (London: The Stationery Office, 2018); Michael Levi, 'Organized Frauds and Organizing Frauds: Unpacking the Research on Networks and Organization', *Criminology and Criminal Justice* (Vol. 8, No. 4, 2008), pp. 389–419.
8. See, for example, Frank Perri and Richard Brody, 'The Dark Triad: Organized Crime, Terror and Fraud', *Journal of Money Laundering Control* (Vol. 14, No. 1, 2011), pp. 53–56; Michael Freeman, 'The Sources of Terrorist Financing: Theory and Typology', *Studies in Conflict and Terrorism* (Vol. 34, No. 6, 2011), pp. 465–71.

The Terrorism Financing Fraud Typology

The association between terrorism financing and fraud has been identified by Europol, the IMF, the FATF, the National Commission on Terrorist Attacks, the UN and the US Department of the Treasury.⁹ However, these sources only provide evidence of a generic association between terrorism financing and fraud. In order to enhance our understanding of the link between terrorism financing and fraud, it is necessary to conduct a more detailed review of the literature and judicial precedent.

Immigration Fraud and Identify Theft

Identity theft provides a useful starting point from which to map the relationship between terrorism financing and fraud. Identity theft, according to the FBI, is ‘a key catalyst fuelling many [terrorism financing] methods’.¹⁰ The association between identity theft and terrorism financing is associated with the attacks on the World Trade Center

in 1993 and 2001.¹¹ The 9/11 Commission noted that ‘all but one of the 9/11 hijackers acquired some form of US identification document, some by fraud’.¹² Norman Willox and Thomas Regan went a step further and concluded that *all* of the 9/11 terrorists were involved in some type of identity theft.¹³ Convictions for terrorism financing in the US include Mahmoud Youssef Kourani, Mohamad Youssef Hammoud and Barry Walter Bujol Jr.¹⁴ Within the UK, Ciaran Maxwell pleaded guilty to preparation of terrorist acts, possession of a controlled drug and possession of articles to use in fraud. Here, the defendant ‘took images of other people’s bank cards and identity documents when he had access to them whilst they were on operations. He did so with the intention of using them in online [identity] fraud’.¹⁵ Other convictions for identity theft and immigration fraud included Abderrahman Bouanane who was living illegally in Finland and using a false identity.¹⁶ These cases illustrate that the first stage for a terrorism financier to obtain access to funding is to commit immigration fraud to illegally enter a country.¹⁷

9. Europol, ‘European Union Terrorism Situation and Trend Report 2017’, 2018, p. 12; IMF, ‘Anti-Money Laundering/Combating the Financing of Terrorism – Topics’; Laura Donohue, ‘Anti-Terrorist Finance in the United Kingdom and United States’, *Georgetown Law Faculty Publications and Other Works* (2006), pp. 315–16; Keith Maguire, ‘Fraud, Extortion and Racketeering: The Black Economy in Northern Ireland’, *Crime, Law and Social Justice* (Vol. 20, No. 4, 1993), pp. 273–92; FATF, ‘Terrorist Financing’; National Commission on Terrorist Attacks Upon the United States, ‘Monograph on Terrorist Financing’, 2004, p. 19; UN Office on Drugs and Crime (UNODC), ‘Digest of Terrorist Cases’, 2010, p. 32; US Department of the Treasury, ‘National Terrorist Financing Risk Assessment 2015’, 2015, p. 16.
10. See Dennis M Lormel, Terrorist Financial Review Group, testimony before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information, 9 July 2002; UNODC, ‘Economic Fraud and Identity Related Crime’; Neil Robinson et al., ‘Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report’, June 2011, p. 18.
11. 9/11 Commission, ‘The 9/11 Commission Report’, 2004, p. 72. The relationship between immigration fraud and terrorism financing was illustrated by the conviction of Ibrahim Elgabrowni for using false passports. He was a messenger during the 1993 World Trade Center attack.
12. 9/11 Commission, ‘The 9/11 Commission Report’, p. 390.
13. Norman Willox and Thomas Regan, ‘Identity Fraud: Providing a Solution’, *Journal of Economic Crime Management* (Vol. 1, No. 1, 2002), pp. 1–15.
14. See US Immigration and Customs Enforcement, ‘Mohamad Youssef Hammoud Sentenced to 30 Years in Terrorism Financing Case’, press release, 27 January 2011; US Department of Justice, ‘Texas Man Gets Max for Attempting to Provide Material Support to Al Qaeda’, 24 May 2012, <<https://www.justice.gov/archive/usao/txs/1News/Releases/2012%20May/120524%20Bujol.html>>, accessed 21 September 2020. Others who were convicted include Colleen LaRose and Jamie Paulin Ramirez, Amer Sinan Alhaggai and Naif Abdulaziz M Afallaj.
15. The Queen vs. Ciaran Maxwell, ‘Sentencing Remarks of Mr Justice Sweeney’, 31 July 2017, <<https://www.judiciary.uk/wp-content/uploads/2017/07/r-v-ciaran-maxwell-sentencing.pdf>>, accessed 1 October 2020.
16. Eurojust, ‘Terrorism Convictions Monitor’, No. 32, December 2018, p. 10; Jussi Rosendahl, ‘Knife Attacker Sentenced to Life in Finnish Court’, 15 June 2018.
17. See Martin Rudner, ‘Misuse of Passports: Identity Fraud, the Propensity to Travel, and International Terrorism’, *Studies in Conflict and Terrorism* (Vol. 3, No. 2, 2018), pp. 95–110.

Credit Card, Personal Loan and Bank Fraud

The second type of fraud associated with terrorism financing is a combination of credit card, personal loan and bank fraud. Related convictions in the US included Khalid Awan and Zoobia Shahnaz.¹⁸ The use of personal loan fraud was illustrated by the 7/7 bombings in London in 2005.¹⁹ The government report concluded that this terrorist cell was ‘self-financed’ and that one of the terrorists, Mohammad Sidique Khan, ‘appears to have provided most of the funding ... [by] credit cards and a £10,000 personal loan. [Khan] defaulted on his personal loan repayments and was overdrawn on his accounts’.²⁰ Furthermore, Bilal Abdullah and Kafael Ahmed funded a terrorist attack in Scotland by fraudulent loans credit cards.²¹ Amedy Coulibaly funded an act of terrorism in Paris after securing a bank loan by using a fraudulent payslip.²² Syed Rizwan Farook and Tashfeen Malik fraudulently obtained a loan prior to committing a terrorist attack in San Bernardino.²³ Mohammed Rehman and Sana Ahmed Khan were convicted of preparing acts of terrorism and possessing articles for terrorist purposes.²⁴ This planned attack was funded by payday loans.²⁵ Ghulam Hussain pleaded guilty to two terrorism-related offences after he

discussed his intention with an undercover police officer to travel to Syria to fight for the Islamic State, and how he had obtained funding for the trip by ‘fraudulently applying for credit cards’.²⁶ The ability of terrorism financiers to obtain access to this part of the typology is exacerbated by convenient credit.²⁷ Examples of convenient credit which terrorism financiers could exploit include non-commercial and commercial cash loans, credit tied to the purchase of goods and payday lenders.²⁸ The ease with which terrorism financiers could secure convenient credit is illustrated by research published by Citizens Advice, which concluded that credit card companies are lending ‘too freely’. The research concluded that approximately 6 million people received a credit limit increase without asking for it from their credit card providers.²⁹ Therefore, Ranstorp took the view that ‘[terrorist] recruits with good credit histories and those well placed to defraud financial institutions, as well as those with a network of contacts willing to provide funds, are particularly prized’.³⁰ Some terrorism financiers have used false identities to obtain funds via credit card, personal loan and bank fraud. This clearly illustrates the link between the first and second parts of the fraud typology.

-
18. See FBI, ‘Khalid Awan Re-Sentenced to 14 Years’ Imprisonment for Providing Material Support and Resources to Indian Terrorist Organization’, 3 April 2012, <<https://archives.fbi.gov/archives>>, accessed 25 June 2020; US Department of Justice, ‘Long Island Woman Sentenced to 13 Years’ Imprisonment for Providing Material Support to ISIS’, press release, 13 March 2020, <<https://www.justice.gov/opa/pr/long-island-woman-sentenced-13-years-imprisonment-providing-material-support-isis>>, accessed 26 June 2020.
 19. See HM Government, *Report into the London Terrorist Attacks on 7 July 2005* (London: The Stationery Office, 2006).
 20. HM Government, *Report of the Official Account of the Bombings in London on 7th July 2005* (London: The Stationery Office, 2005), p. 23. For a more detailed discussion of the case, see Lewis Herrington, ‘British Islamic Extremist Terrorism: The Declining Significance of Al-Qaeda and Pakistan’, *International Affairs* (Vol. 91, No. 1, 2015), pp. 17–35, 29–30.
 21. Tom Keatinge and Florence Keen, ‘Lone-Actor and Small Cell Terrorist Attacks: A New Front in Counter-Terrorist Finance?’, *RUSI Occasional Papers* (January 2017), p. 13.
 22. *BBC News*, ‘Paris Attacks: Investigators Turn up New Leads’, 19 January 2015.
 23. The loan was paid to Farook by Proper, a California-based online lender. See Dan Whitcomb and Edward McAllister, ‘California Shooters Borrowed £28,000 Before Attack: Source’, 9 December 2015; US Department of Justice, ‘“Wife” of Man Facing Charges of Conspiring with Shooter in San Bernardino Attack Pleads Guilty to Entering into Sham Marriage’, press release, 26 January 2017, <<https://www.justice.gov/usao-cdca/>>, accessed 27 May 2020.
 24. Terrorism Act 2006 (UK), section 5; Terrorism Act 2000 (UK), section 57. Sana Ahmed Khan’s sentence was reduced on appeal to 23 years. *BBC News*, ‘“Silent Bomber” Plotter Who Planned London Terror Attack Has Sentence Cut’, 18 May 2016.
 25. *BBC News*, ‘“Silent Bomber” Plotter Who Planned London Terror Attack Has Sentence Cut’.
 26. Crown Prosecution Service, ‘R v Ghulam Hussain (2017)’, <<https://www.cps.gov.uk/counter-terrorism-division-crown-prosecution-service-cps-successful-prosecutions-2016>>, accessed 14 July 2020.
 27. See Nicholas Ryder and Rachel Thomas, ‘Convenient Credit And Consumer Protection – A Critical Review of the Responses of Labour and Coalition Governments’, *Journal of Social Welfare and Family Law* (Vol. 33, No. 1, 2011), pp. 85–95; Nicholas Ryder, Margaret Griffiths and Lachmi Singh, *Commercial Law: Principles and Policy* (Cambridge: Cambridge University Press, 2012).
 28. For example, the ‘Birmingham rucksack bomb plot’. See David Anderson, *The Terrorism Acts in 2012* (London: The Stationery Office, 2013), p. 26; *Evening Standard*, ‘Would Be Suicide Bombers Tried to Fund Terror Plot with Payday Loans’, 24 October 2012.
 29. Citizens Advice, ‘Uninvited Credit Limit Increases Push People Further into Debt’, 17 November 2017.
 30. Magnus Ranstorp, ‘Microfinancing the Caliphate: How the Islamic State is Unlocking the Assets of European Recruits’, *CTC Sentinel* (Vol. 9, No. 5, 2016), p. 11.

Tax Fraud

Tax fraud is a frequently used method of terrorism financing. For example, in the US, tax fraud convictions associated with terrorism financing include Pedrouz Sedaghaty and Soliman Hamd Al-Buthe,³¹ and Emadeddin Muntasser, Muhammed Mubayyid and Samir al-Monla.³² There is evidence to suggest that terrorism financiers in Europe have used tax fraud to obtain funding. For example, Europol stated, ‘in Spain, members of a terrorist cell were engaged in value-added tax and other fraud in different parts of the EU to fund the cost of travelling to conflict areas’.³³ Tax fraud is an important funding avenue for terrorists in the UK.³⁴ For example, the Ulster Volunteer Force (UVF), the Ulster Defence Association (UDA) and the IRA exploited loopholes relating to tax exemption status. The Inland Revenue lost £7 million in tax revenue, the UVF and UDA each earned £1.5 million, while the IRA accrued £28.5 million.³⁵ In 2015, Thomas Murphy, who is regarded as a key terrorism financier for the IRA, was convicted of tax evasion in the Republic of Ireland and sentenced to two years’ imprisonment.³⁶ Although there are no reported tax fraud convictions relating to terrorism financing in the UK, it has been suggested that Al-Qa’ida has secured funding via this method. For example, *The Times* reported that UK taxpayer money had

been used to fund acts of terrorism including terrorist attacks in London.³⁷ The report suggests that £80 million was funnelled to Al-Qa’ida representatives in Pakistan and Afghanistan.³⁸ In 2003, HMRC connected these frauds with Shehzad Tanweer, one of the terrorists who detonated his improvised explosive device on the Aldgate train in 2005, yet it appears that the information was not disclosed to law enforcement agencies or the UK Security Services.³⁹ There are two important points to note here. First, the monies which terrorist groups have obtained via tax fraud are higher than those acquired by the first two parts of the typology. Second, VAT fraud has been a staple funding avenue for terrorist groups in the UK.

Student Loan Fraud

A recent development in the evolution of terrorism financing and fraud is the misuse of student loans. The FATF highlighted how terrorism financiers in the Netherlands had acquired funding from student benefits.⁴⁰ Tom Keatinge and Florence Keen argue that student loans are ‘ideal for the limited costs associated with lone actor or small cell attacks’.⁴¹ Florence Gaub and Julia Lisiecka note that ‘in the UK ... jihadists have funded their trips with student loans’.⁴² Examples for this part of the typology

-
31. See *US vs. Mubayyid*, United States Court of Appeals, First Circuit, 1 September 2011, 658 F.3d 35.
 32. US Department of Justice, ‘Former Officers of a Muslim Charity, Care International, Inc., Convicted’, press release, 11 January 2008, <https://www.justice.gov/archive/opa/pr/2008/January/08_nsd_021.html>, accessed 18 September 2020. Further examples include: Johnathan Paul Jimenez; Michael Todd Wolf; and Hossein Lahiji, Najmeh Vahid Dasterjerdi and Houcine Becher Ghoul.
 33. Europol, ‘European Union Terrorism Situation and Trend Report 2016’, 2017, p. 12. Also, see Europol, ‘Counter-Terrorist Operation: Spanish National Police Disrupts Criminal Organisation Which Finances Al-Qaeda’, press release, 19 June 2019, <<https://www.europol.europa.eu/newsroom/news/counter-terrorist-operation-spanish-national-police-disrupts-criminal-organisation-which-financed-al-qaeda>>, accessed 18 June 2020. Pedro Felício, head of Europol’s economic operations and property crime unit, provided three examples of how tax fraud has been used by terrorism financiers. First, in Sweden and Denmark, a tax-fraud scheme worth £8.5 million was believed to have funded Al-Qa’ida. Second, the German police disrupted a £54-million VAT fraud scheme for terrorist groups in 2015. Finally, information found in a cave in Pakistan that was used by Osama bin Laden as a hideout led investigators to a criminal network based in Italy that stole £900 million through VAT fraud on CO₂ certificates. See European Parliament, ‘Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance Ordinary Meeting’, 28 June 2018, <<https://multimedia.europarl>>, accessed 30 June 2020.
 34. John Horgan and Max Taylor, ‘Playing the “Green Card” – Financing the Provisional IRA: Part 1’, *Terrorism and Political Violence* (Vol. 11, No. 2, 1999), p. 8.
 35. Andrew Silke, ‘In Defense of the Realm: Financing Loyalist Terrorism in Northern Ireland – Part One: Extortion and Blackmail’, *Studies in Conflict and Terrorism* (Vol. 21, No. 4, 1998), p. 349.
 36. The conviction and sentence of 18 months was upheld in the Court of Appeal. See *BBC News*, ‘Who is Thomas ‘Slab’ Murphy?’, 26 February 2016.
 37. Tom Harper, ‘Taxman Kept Quiet While £8bn Fraud Helped Fund Osama bin Laden’, *The Times*, 30 March 2019.
 38. Sara Elizabeth Williams, ‘£80m of British Taxpayers’ Money “Funnelled to Al-Qaeda” in Decades-Long Scam’, *The Telegraph*, 31 March 2019.
 39. It has been reported that Shehzad Tanweer left £121,000 in his will, even though he worked on a part-time basis in a fish and chip shop. See Sophie Goodchild, ‘The Mystery of the London Bomber and His Secret Wealth’, *The Independent*, 8 June 2006. HMRC became aware of the tax fraud scheme as early as 1995. See Wadood Mushtaq, ‘Imran Hussain’s Father Says Not Responsible for Scottish-Pakistani Son’s £300m Fraud’, *Geo News*, 24 November 2019, <<https://www.geo.tv/>>, accessed 22 June 2020.
 40. FATF, ‘Terrorist Financing in West and Central Africa’, p. 25.
 41. Keatinge and Keen, ‘Lone-Actor and Small Cell Terrorist Attacks’, p. 13.
 42. Florence Gaub and Julia Lisiecka, ‘The Crime–Terrorism Nexus’, European Union Institute for Security Studies, 12 April 2017.

include Taimour Abdulwahab, Yahya Rashid and Salman Abedi.⁴³ The use of student loans echoes the problems associated with credit fraud and despite the small number of cases, the threat posed by this part of the funding model must not be underestimated.

Insurance Fraud

Insurance fraud is another mechanism by which terrorism financiers have acquired funding, with reported cases in the US and Germany.⁴⁴ The FATF reported that these fraudulent insurance schemes are referred to as ‘crash for cash’ and often involve fraudsters deliberately crashing into vehicles of innocent motorists or submitting false claims for accidents. The FATF highlighted several instances in Spain where terrorism financiers committed frauds by faking traffic accidents and hiring bogus policies. The FATF stated that terrorism financiers ‘needed to obtain funds quickly ... by faking numerous and rough traffic accidents which exposed them to detection’.⁴⁵ The threat posed by fraudulent insurance claims was recognised in the 2017 National Risk Assessment where ‘individuals ... falsely claim to have been defrauded or where individuals apply for a loan under false pretences’.⁴⁶ Collins noted that ‘insurance fraud also offers some rich possibilities ... the IRA bombed many businesses in Northern Ireland, with

the compliance of the business owners, so that the owners could claim the resulting insurance’.⁴⁷

Non-Profit Organisations

One of the most documented examples of fraud used by terrorism financiers are non-profit organisations (NPOs).⁴⁸ The FATF reported that Al-Qa’ida, the Liberation of Tamil Eelam and the Islamic State have used NPOs.⁴⁹ They added that terrorism financiers have used NPOs in Belgium, the UK, Russia and the US to obtain access to funding.⁵⁰ Related terrorism financing convictions include the former leaders of the Holy Land Foundation, Naseer and Khalid Ali and Mohammed and Shafiq Ali.⁵¹ The use of misapplied charitable donations and the targeting of NPOs is one of the most commonly used parts of the terrorism financing typologies. Research has suggested that this funding mechanism is one of the central funding mechanisms used by many terrorist groups.⁵²

Mortgage Fraud

The connection between terrorism financing and mortgage fraud is difficult to detect.⁵³ However, there are several instances in the US that illustrate the link including

-
43. On Taimour Abdulwahab, see *The Local*, ‘Suicide Bomber Lived Off Swedish Student Aid’, 18 February 2013, <<https://www.thelocal.se/20130218/46250>>, accessed 17 September 2020. On Yahya Rashid, see *R v Yahya Rashid*, 2016, EWCA Crim 568. The court stated, ‘On 25 February 2015 Rashid purchased flights for Morocco for himself, Khalid Abdul-Rahman, Ibramim Amouri, Swaleh Mohamed and Deqo Osman, Swach Mohamed’s wife at a total cost of £906. It appears that the funds were derived from the student loan he had obtained’. On Salman Abedi, see Robert Mendick, ‘Exclusive: Manchester Suicide Bomber Used Student Loan and Benefits to Fund ‘Terror Plot’’, *The Telegraph*, 27 May 2017.
44. Insurance Fraud News, ‘Terrorism and Insurance Fraud “Significantly Linked”, Says British Experts’, 6 November 2014, <https://insurancefraud.org/news_archives/terrorism-and-insurance-fraud-significantly-linked-says-british-experts/>, accessed 22 May 2020; John Kane and April Wall, ‘Identifying the Links Between White-Collar Crime and Terrorism’, April 2015, <<https://www.ncjrs.gov/pdffiles1/nij/grants/209520.pdf>>, accessed 22 June 2020; *New York Times*, ‘German Court Convicts Three Men of Aiding Al Qaeda’, 5 November 2007.
45. See FATF, ‘Terrorist Financing in West and Central Africa’, p. 16.
46. HM Government, *National Risk Assessment of Money Laundering and Terrorist Financing 2017* (London: The Stationery Office, 2017), p. 32.
47. See Silke, ‘In Defense of the Realm’, p. 122.
48. For a more detailed discussion, see Peter Romaniuk and Tom Keatinge, ‘Protecting Charities from Terrorists ... and Counter-Terrorists: FATF and the Global Effort to Prevent Terrorist Financing Through the Non-Profit Sector’, *Crime, Law and Social Change* (Vol. 69, No. 2, 2018), pp. 265–82; Clive Walker, ‘Terrorism Financing and the Policing of Charities: Who Pays the Price?’, in Colin King and Clive Walker (eds), *Dirty Assets: Emerging Issues in the Regulation of Criminal and Terrorist Assets* (London: Routledge, 2014).
49. See, for example, FATF, ‘Risk of Terrorist Abuse in Non-Profit Organisations’, June 2014, p. 18; FATF, ‘Financing of the Terrorist Organisation Islamic State in Iraq and the Levant’, pp. 18–20.
50. See FATF, ‘Terrorist Financing’, pp. 12–13.
51. FBI, ‘No Cash for Terror: Convictions Returned in Holy Land Case’, 25 November 2008, <<https://archives.fbi.gov/archives>>, accessed 15 July 2020. For a more detailed discussion, see Jeroen Gunning, ‘Terrorism, Charities, and Diasporas’, in Thomas Biersteker and Sue Eckert (eds), *Countering the Financing of Terrorism* (London: Routledge, 2008), pp. 93–125; *R. v. Nasser et al.* (Irfan Nasser), 2012, EWCA Crim. 2; *BBC News*, ‘Ali Twins Jailed for Funding Terrorism Abroad’, 1 August 2012.
52. See Gurule, *Unfunding Terror*.
53. FATF, ‘Money Laundering and Terrorist Financing Through the Real Estate Sector’, June 2007, p. 5. See also Perri and Brody, ‘The Dark Triad’, p. 53.

Ahmad Jebril and Nemr Ali Rahal.⁵⁴ Nonetheless, the FATF were able to provide a number of instances where mortgage fraud was used by terrorism financiers in Belgium and Spain.⁵⁵ There are no reported convictions of mortgage fraud associated with terrorism funding in the UK. However, some have noted that ‘mortgage fraud is being used a lot by organised rings to provide safe housing for organised criminals and terrorists’.⁵⁶ In 2008, the Association of Chief Police Officers reported that there was no evidence of mortgage fraud directly funding acts of terrorism, but that mortgage fraud could be used to fund safe houses.⁵⁷ Indeed, the FATF stated that because of an investigation by the UK financial intelligence unit, the police were able to identify terrorism financiers who had engaged in mortgage fraud.⁵⁸

Benefit Fraud

Benefit fraud is one of the most frequently identified frauds linked with terrorism financing. The FATF has identified foreign terrorist fighters who have used benefit fraud,⁵⁹ particularly in the Netherlands,⁶⁰ Denmark,⁶¹ Sweden⁶² and France.⁶³ The Swedish Defence University stated that citizens who travelled to join the Islamic State financed their trips ‘through the misuse of social welfare allowance and other state benefits’.⁶⁴ In June 2012, Munir Awad was convicted of planning to commit a terrorist attack in Denmark which was funded by ‘sickness benefits’.⁶⁵

Mohammed Merah, who killed seven people in France, stated that his only income was ‘state benefits worth €475 a month’.⁶⁶ In June 2016, Nader Elhuzayel and Muhanad Badawi were convicted of attempting to provide material support to the Islamic State and aiding and abetting the attempt to provide support to the Islamic State. Elhuzayel was guilty of 26 counts of bank fraud, and Badawi was found guilty of federal financial aid fraud.⁶⁷ In November 2019, Guled Omar was convicted for conspiring to provide material support to ISIL by attempted financial aid fraud.⁶⁸

Conclusions

Fraud is a popular method for financing terrorist attacks and this paper has identified a terrorism financing fraud typology. Frequently used methods in Europe are benefit fraud, credit card/personal loan/bank fraud, NPO fraud and tax fraud. It is difficult to determine which type of fraud within the typology is the most frequently used, which are declining in usage and which are becoming more popular. What is not in doubt is that fraud continues to be used to support terrorist groups and autonomous terrorist entities across Europe. Terrorists have exploited the benefits afforded by the EU to its citizens, including access to credit, manipulated welfare payments and exposed loopholes in the funding of higher education. Furthermore, one recent study has illustrated the connections between cryptoassets, social media platforms

-
54. *The Telegraph*, ‘US Hate Preacher Who “Inspired” London Terror Attackers Is Convicted Fraudster’, 7 June 2017; US v Nemr Ali Rahal, 2006, Case No. 05-CR-80476.
55. FATF, ‘Money Laundering and Terrorist Financing Through the Real Estate Sector’, pp. 9, 22–24.
56. Mortgage Strategy, ‘Mortgage Expo 2008: Mortgage Fraud is Funding Terrorism’, 14 May 2008, <<https://www.mortgagestrategy.co.uk/news/mortgage-expo-2008-mortgage-fraud-is-funding-terrorism/>>, accessed 26 June 2020.
57. *BBC News*, ‘Mortgage Fraud is Funding Crime’, 5 March 2008.
58. FATF, ‘Terrorist Financing’, p. 30.
59. FATF, ‘Terrorist financing in West and Central Africa’, p. 24.
60. *Ibid.*, p. 25; Ranstorp, ‘Microfinancing the Caliphate’, p. 13; Norwegian Defence Research Establishment, ‘The Financing of Jihadi Terrorist Cells In Europe’, 5 February 2015, p. 23.
61. FATF, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Denmark: Mutual Evaluation Report’, August 2017, p. 35; Statsadvokaten, ‘Money Laundering in Denmark: National Risk Assessment 2015’, 2015.
62. See FATF, ‘Anti-Money Laundering and Counter-Terrorist Financing Measures: Sweden: Mutual Evaluation Report’, April 2017, p. 90; Swedish Government, ‘National Risk Assessment of Money Laundering and Terrorist Financing in Sweden’, 2019.
63. See Jack Moore, ‘French Government Paid ISIS Fighters Social Security While They Were in Syria’, 26 October 2017.
64. Magnus Normark, Magnus Ranstorp and Filip Ahlin, ‘Financial Activities Linked to Persons from Sweden and Denmark Who Joined Terrorist Groups in Syria and Iraq During the Period 2013–2016’, Center for Asymmetric Threat Studies and Swedish Defence University, 1 February 2017.
65. See Norwegian Defence Research Establishment, ‘The Financing of Jihadi Terrorist Cells In Europe’, p. 23; *BBC News*, ‘Four Guilty of Danish Plot over Muhammad Cartoons’, 4 June 2012.
66. Norwegian Defence Research Establishment, ‘The Financing of Jihadi Terrorist Cells In Europe’, p. 37.
67. US Department of Justice, ‘Two Orange County Men Convicted of Conspiring to Join ISIL; They Also Engaged in Fraud to Finance One’s Trip to Syria’, press release, 21 June 2016, <<https://www.justice.gov/usao-cdca/pr/two-orange-county-men-convicted-conspiring-join-isil-they-also-engaged-fraud-finance>>, accessed 18 June 2020.
68. US Department of Justice, ‘Nine Twin Cities Men Sentenced For Providing Material Support To ISIL’, press release, 16 November 2016, <<https://www.justice.gov/usao-mn/pr/nine-twin-cities-men-sentenced-providing-material-support-isil>>, accessed 18 June 2020.

and fraud.⁶⁹ Fraud has become a common and easy funding mechanism for disparate terrorist entities. The approach towards investigating and prosecuting suspected instances of fraud and terrorism financing varies between countries. For example, the UK approach is hampered by an inconsistent enforcement prosecutorial stance from the Crown Prosecution Service. A review of terrorism-related prosecutions between 2016 and 2019 illustrates that out of 114 convictions, only three were related to fraud.⁷⁰ By contrast, in the US, law enforcement agencies have used fraud investigations, arrests and prosecutions to disrupt terrorists.

Nicholas Ryder is a professor of financial crime and head of research at Bristol Law School at the University of the West of England, Bristol.⁷¹

-
69. Nicholas Ryder, 'Cryptoassets, Social Media Platforms and Defence Against Terrorism Financing Suspicious Activity Reports: A Step into the Regulatory Unknown', *Journal of Business Law* (Vol. 8, 2020), pp. 668–93.
70. Crown Prosecution Service, 'The Counter-Terrorism Division of the Crown Prosecution Service (CPS) – Successful Prosecutions Since 2016', <<https://www.cps.gov.uk/crime-info>>, accessed 13 October 2020.
71. The author would like to thank Connor Bayley (Cardiff University), Charlie Robson and Sam Bourton (University of the West of England, Bristol) for their invaluable help with the research on this project.



Financing Right-Wing Extremism and Terrorism

Bethan Johnson

About Project CRAFT

Project CRAFT 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 CRAFT is funded by the European Union'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 <projectcraft.eu>.

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

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



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <<http://creativecommons.org/licenses/by-nc-nd/4.0/>>.

Introduction

If ideology is at the heart of extremism and terrorism, then money is its lifeblood. Without money, ideas may well remain simply that. As the adage goes, ‘money talks’ – but only through the combination of ideas and capital can violent extremists coalesce and disseminate their beliefs, plot and carry out attacks. In the last decade, there has been an exponential growth in right-wing extremism and terrorism around the globe. What was once considered a ‘very low risk to national security’ is now classified as a clear and present danger, with every major Western intelligence community and many supranational bodies, including the UN, noting the increasing threat from the extreme right-wing.¹ Money has played an important role, and this paper analyses how those advocating extreme right-wing violence operate financially. Through such analysis, an appropriate response can be developed.

This paper focuses on the financing of right-wing extremism and terrorism, but within the umbrella terms are myriad different categorisations. For instance, mass media and scholarship use terms including ‘alt-right’, ‘radical right’, ‘far right’, and ‘right-wing extremism’ interchangeably, but these typologies fail to capture important ideological and operational distinctions. Moreover, ‘extremism’ and ‘terrorism’ represent two different, though not disparate, phenomena, not least in the legal sense.² Terminological decisions, therefore, need to be explicit rather than implicit for the forthcoming research to be appropriately understood and used. The research and recommendations of this paper relate specifically to the financing of right-wing extremism and terrorism in the context of neo-Nazism, neo-fascism, accelerationism, white supremacy, white separatism, identitarianism, and the Christian Identity movement.³ In charting the financial practices

of extremist and terrorist groups, this paper concentrates on practices employed by government-designated terrorist groups, as well as organisations, militia movements and individuals that openly promote the use of violence for the radical overthrow or reform of the state or global order. As right-wing extremism and terrorism is a global phenomenon that operates irrespective of borders – and has killed hundreds of people across multiple continents in recent years – this paper makes a conscious effort to discuss the financing methodologies at play in various geographical contexts.

A significant proportion of the available scholarship on right-wing extremism and terrorism is ‘concerned with societal factors that lead to radicalisation—but there has been as yet no attempt to understand how these individuals and groups raise funds, in contrast to the focus applied to the financing of Islamist terrorist actors.’⁴ This gap has begun to be addressed,⁵ but, nevertheless, a sustained, focused examination of the financial transactions of the multiplicity of extreme right actors (not only terrorists, but also extremists more broadly) has not been offered.

Analysis of extreme right funding has significant ramifications for counterterrorism efforts. Certain right-wing extremists and terrorists draw inspiration from groups such as the Islamic State and Al-Qa’ida and there is some overlap in their financial practices. However, there are differences. Applying identical counterterrorism financial policies to extreme-right and Islamist terrorists alike has not and will not prove sufficient to prevent violence and halt recruitment. Certain measures work to stem the tide of various forms of terrorism, but to address the rising threat specific attention needs to be paid to how those on the extreme right-wing fund themselves.

1. UN Security Council Counter-Terrorism Committee, ‘Member States Concerned by the Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism’, CTED Trends Alert, April 2020’, 19 March 2019, <<https://homeofficemedia.blog.gov.uk/2019/03/19/factsheet-right-wing-terrorism/>>, accessed 12 November 2020; Vikram Dodd and Jamie Grierson, ‘Fastest-Growing UK Terrorist Threat Is from Far Right, Say Police’, *The Guardian*, 19 September 2019; Nikolaj Nielsen, ‘Internal EU Report: Far-Right Terrorist Attacks Rise’, *Euobserver*, 11 May 2020, <<https://euobserver.com/justice/148311>>, accessed 12 November 2020; Europol, ‘Terrorism in the EU: Geographically Widespread and Multifaceted’, press release, 23 June 2020, <<https://www.europol.europa.eu/newsroom/news/terrorism-in-eu-geographically-widespread-and-multifaceted>>, accessed 12 November 2020; Willem Marx, ‘Jihadist Plots Used to Be U.S. and Europe’s Biggest Terrorist Threat. Now It’s the Far Right’, *NBC News*, 27 July 2020; New Zealand Security Intelligence Service, ‘2019 Annual Report’, <<https://www.nzsis.govt.nz/assets/media/NZSIS-Annual-Report-2019.pdf>>, accessed 12 November 2020.
2. Crown Prosecution Service, ‘Terrorism’, <<https://www.cps.gov.uk/crime-info/terrorism>>, accessed 17 November 2020.
3. This thereby excludes what may justifiably be identified as ‘right-wing extremism’ or ‘terrorism’ in relation to single-issue groups, such as those in the anti-abortion movement or militant anti-LGBTQ+ rights campaigners.
4. Tom Keatinge, Florence Keen and Kayla Izenman, ‘Fundraising for Right-Wing Extremist Movements’, *RUSI Journal* (Vol. 164, No. 2, 2019), p. 12.
5. Jessica Davis, ‘New Technologies But Old Methods in Terrorism Financing’, Project CRAFT, Research Briefing No. 2, 2020, <<https://static1.squarespace.com/static/5e399e8c6e9872149fc4a041/t/5f18579880818c6feb0e6a49/1595430886467/CRAAFT+Jessica+Davis.pdf>>, accessed 12 November 2020.

Group Fundraising

Those on the extreme right-wing have used a variety of group structures over the last century, from networks with thousands of members to small, regional cells of under 10 people. As a result, methods of raising funds vary, but patterns can be found among major groups around the world. One traditional source of funding has been membership fees, or ‘tithes’ in the case of certain Christian Identity groups, that an affiliated individual is expected to pay annually to help sustain the group’s efforts. Groups including the Ku Klux Klan also allegedly charge an application fee.⁶ Relatedly, group paraphernalia including flags and clothing also provides a major source of revenue – KKK robes, for example, are sold at a high cost to members.⁷

They also derive revenue from producing online content, via videos with advertisements on mainstream platforms or exclusive material hidden behind paywalls. Although efforts have been made by many platforms to demonetise radical content, for years this served as a means of fundraising. Extreme right-wing groups also try to crowdfund online, which can prove exceptionally profitable.⁸ One report found that fundraising for the legal defence of the creator of neo-Nazi website *The Daily Stormer* raised more than \$150,000.⁹

Music represents another major source of funding for those on the extreme right. Not only are graphic, radical lyrics potentially significant radicalising agents, but merchandising including CDs, radio broadcasts, band t-shirts and concert tickets, are all lucrative. In particular, money is made through the hosting of music concerts and multi-day

festivals focusing on ‘death metal’ and white power bands. These events have been held all over Europe and North America, either one-off events or annual gatherings marking important dates for the extreme right.¹⁰ Examples of the largest events include the annual Rock Against Foreign Inundation and Rock for Identity in Germany and the Asgardrei Festival in Ukraine, though there are hundreds of smaller concerts spread across white-majority countries.¹¹ With bands from around the world, these events attract international audiences. Event organisers raise funds not only directly through ticket sales (which can cost hundreds of pounds, especially VIP or special access tickets), but also through massively inflating prices on food and drink. While the cost of hosting such events may be high in the case of multi-day, international concerts, they can net organisers anywhere from €100,000 to €250,000.¹²

Martial arts and tactical training is yet another burgeoning revenue stream. There has been a growing trend for combining music festivals with ‘fight nights’, part of a broader push to incorporate physical training into mass gatherings.¹³ Venues in Russia have become particularly popular given its lax stance on paramilitaries, though there are smaller-scale programmes in various countries.¹⁴ Groups also raise money via the sale of self-defence equipment and ‘doomsday prepping’ kits, particularly to neo-Nazis.¹⁵

Many of these forms of financing have now been hindered by coronavirus pandemic restrictions. While certain strains of right-wing extremism do not see coronavirus as a genuine threat to society and those with an anti-state ideology are sceptical of government guidance, the enforcement of regulations against gatherings have hindered the ability of

6. Brian Palmer, ‘What’s on a Ku Klux Klan Membership Application’, *Slate*, 8 August 2012; The Anti-Defamation League, ‘Aryan Nations/Church of Jesus Christ Christian’, <<https://www.adl.org/education/resources/profiles/aryan-nations>>, accessed 12 November 2020.
7. Rosie Cima, ‘How the KKK Scammed its Members for Cash’, *Priceonomics*, <<https://priceonomics.com/when-the-klk-was-a-pyramid-scheme/>>, accessed 12 November 2020.
8. Davis, ‘New Technologies But Old Methods in Terrorism Financing’.
9. Erin Carson, ‘Here’s Where Nazi Sympathizers Go to Raise Money’, *CNET*, 4 December 2017, <<https://www.cnet.com/news/neo-nazi-sympathizers-crowdfunding/>>, accessed 12 November 2020.
10. For example, Hitler’s birthday, the dates of Nazi invasions of different countries or the death dates of ‘martyrs’ of the movement.
11. In the German state of Thuringia alone, 60 are held annually. See Erika Solomon, ‘The Dangers of a Neo-Nazi Woodstock’, *The Atlantic*, 12 October 2018; Michael Colborne, ‘The Upcoming Neo-Nazi Concert in Ukraine That No One Is Talking About’, *Haaretz*, 18 June 2019; Bernhard Forchtner, ‘Fancy a Show? Neo-Nazi Concerts in Germany’, Centre for Analysis of the Radical Right, 24 September 2018; Michael Colborne, ‘Kyiv, Ukraine: A New Hub for International Neo-Nazi Concerts’, Centre for Analysis of the Radical Right, 3 October 2019; Michael Colborne, ‘Neo-Nazis From Across Europe Rally in Budapest’, *Al Jazeera*, 8 February 2020.
12. Solomon, ‘The Dangers of a Neo-Nazi Woodstock’.
13. Karim Zidan, ‘RAM’s Revival and the Ongoing Struggle Against MMA’s Far-Right Fight Clubs’, *The Guardian*, 27 November 2019; Karim Zidan, ‘Fascist Fight Clubs: How White Nationalists Use MMA as a Recruiting Tool’, *The Guardian*, 11 September 2018; Christopher Miller, ‘Azov, Ukraine’s Most Prominent Ultranationalist Group, Sets its Sights on U.S., Europe’, *Radio Free Europe*, 14 November 2018.
14. Kristie Pladson, ‘German Neo-Nazis Trained at Russian Camps: Report’, *DW*, 5 June 2020; Hans Pfeifer, Mikhail Bushuev and Vladimir Esipov, ‘Why Are German Neo-Nazis Training in Russia?’, *DW*, 6 June 2020; *Moscow Times*, ‘Russian “Terrorists” Training German Neo-Nazi Youth in Combat – Reports’, 9 June 2020.
15. Katrin Bennhold, ‘Body Bags and Enemy Lists: How Far Right Police Officers and Ex-Soldiers Planned for “Day X”’, *New York Times*, 4 August 2020; Maik Baumgärtner et al., ‘Harmless Stockpilers or Neo-Nazi Survivalists?’, *Spiegel International*, 21 November 2019.

organisers to put on large public events or even to easily meet to plan their next steps.

Lone Actor Fundraising

In the last decade, the majority of extreme right-wing violence and terrorism has been perpetrated by lone actors, in many cases unaffiliated with any specific extremist group. Lone actors killed 77 in Norway in 2011; three at a school in Trollhättan, Sweden in 2015; six at a mosque in Quebec City, Canada in 2017; 51 at two mosques in Christchurch, New Zealand in 2018; 11 at a synagogue in Pittsburgh, Pennsylvania in 2018; 23 at a Walmart in El Paso, Texas in 2019; and nine at shisha bars in Hanau, Germany in 2020. Added to this are hate crimes, non-mass casualty attacks like that in Finsbury Park in 2017 and Macerata in 2018, and the assassination of politicians including British MP Jo Cox and German politician Walter Lübcke. Around the world, lone actor attacks have become the norm for extreme right-wing violence.

Despite what their classification implies, ‘lone’ actors are never truly alone. They plot and perpetrate acts of violence individually, but their radicalisation still relies upon engagement with propaganda produced by others and they often interact with people holding similar beliefs.¹⁶ This has implications not only for understanding the anthropological and psychological elements at play in radicalisation, but also for financing. Lone actors benefit, even if indirectly, from traditional group-funding efforts, as consumers of their print and online content. They also may attend mass gatherings like concerts or martial arts training sessions, or listen to radical music. Such activities may help further solidify the beliefs that motivate their individual acts of violence.

Lone actors have distinctive financial fingerprints, but they still display patterns that are significant for counterterrorism financing policymaking. Lone actors fund their plans via two main revenue streams: individual income from employment; and crowdfunding or public appeals for financial support. There have also been attempts by the extreme right to raise money through buying and selling cryptocurrencies, particularly during the initial bubble.¹⁷

The impact of the coronavirus pandemic upon lone actor terrorist financing is less apparent. With regard to fundraising, lone actors already have fewer financial needs than groups, meaning, barring job-loss, the pandemic’s impact on their ability to fund their activities would likely prove minimal in any *immediate* sense. The pandemic may, in fact, further radicalise individuals in the face of ongoing isolation, global financial strain, the non-Western origin of the virus, governments’ top-down deployment of lockdowns and fines, and a general sense of societal uncertainty. This period may prove a time when lone actors turn inwards, make intricate plans, save money, and prepare for when communities begin to open again.

Spending

Extremist and terrorist groups, as well as lone actors, spend their money on an assortment of items, not all immediately obvious to observers.

Group-facilitated mass gatherings, fight training camps, music production, and printing materials all have considerable overheads. Venues owned by radicalised or sympathetic owners have proven to be cost effective and secure locations for mass gatherings, but typically such large-scale groupings are held in venues at full cost and with the threat of last-minute cancellation if the venue uncovers the beliefs of attendees. This has been of particular concern in recent years as attempts by local communities to stop these types of events (particularly music festivals) have hurt their bottom line. Local governments’ tactic of last-minute revocation of permission has forced groups to change venues with little notification, and caused some to simply abandon them. In one instance, a combined ban on alcohol and the purchase of the remaining alcohol in local shops by town members led to a dry concert, not only reducing the potential for drunken altercations, but also cutting the profitability of the event.¹⁸ Despite such efforts, mass gatherings still provide significant income, which is spent on hosting similar events in subsequent years, and on other, longer-term goals.

Legal fees are another major cost for extremist and terrorist groups. In addition to criminal charges filed against individual members of such groups, there have been multiple successful attempts to sue groups or their

16. See Matthew Feldman, ‘Comparative Lone Wolf Terrorism: Toward a Heuristic Definition’, *Democracy and Security* (Vol. 9, No. 3, 2013), pp. 270–86.

17. David Gerard, ‘Neo-Nazis Bet Big on Bitcoin (and Lost)’, *Foreign Policy*, 19 March 2019.

18. *BBC News*, ‘Beer Ban Leaves German Neo-Nazi Rock Fans Thirsty’, 24 June 2019.

leaders in civil trials. Following a 1999 attack on a mother and child by members of the Aryan Nations group in the US, the Southern Poverty Law Center (SPLC) won a lawsuit that awarded the family a \$6.3-million judgment, an amount so substantial that it forced the Christian Identity-inspired Aryan Nations to sell their compound before the group eventually collapsed.¹⁹ In fact, the SPLC has had considerable success in filing suits on behalf of victims and victims' families, with two active cases at present linked to extremism.²⁰ Several other lawsuits on the grounds of defamation and libel have been and are being brought against extremist and terrorist groups, their media outlets, and specific leaders or individuals.²¹ Fighting such lawsuits and paying judgments are ongoing costs for the movement. Of additional note are the fees such groups accrue through fines: intentional or unintentional flouting of laws (from wearing a swastika in Germany, for example, to failure to obey regulations on marches or rallies) frequently result in fines, if not jail time.²²

Weapons (including guns, bomb materials and knives) are another expenditure for both extreme-right individuals and groups, as are the rentals of cars and trucks used either as weapons or as transport to the site of an attack. The terrorist attack in Halle, Germany that resulted in two deaths in 2019 also demonstrates the use of 3D printing technology in terrorist attacks, as elements of the attacker's weaponry were printed rather than purchased from a regulated vendor.²³ While 3D printers remain relatively expensive and the live-stream footage of the attack evidences some malfunctioning of the weaponry, in the future price and technical difficulties could be addressed and these untraceable weapons could become commonplace.

Smaller purchases may also prove important in attempts at identifying those individuals being radicalised or plotting violence. For instance, several books are popular among those promoting terrorist violence, including Adolf Hitler's

Mein Kampf, James Mason's *Siege*, and William Luther Pierce's *The Turner Diaries*. There are multiple publishing houses selling such books, as well as translations of other extremist texts in multiple languages, reprints of early 20th-century texts, and new content that promotes extreme-right narratives. Reading such texts is viewed as essential by many extremist groups. The Base and Feuerkrieg Division, for example, have recruitment procedures that specifically enquire as to what radical books would-be recruits have read, while the website of Identity Evropa (now known as the American Identity Movement) offered potential recruits a reading list.²⁴

These purchases focus on the short-term goals of violence and radicalisation. However, some within the extreme right are using funds to help realise longer-term plans. Perhaps the most noteworthy of these is the purchase of land. Findings by MOBIT, a Thuringia-based initiative against far-right activity, and German intelligence agencies have shown how the German neo-Nazi movement has a clear strategy that involves the purchase of land, often in the eastern states. In the state of Saxony, neo-Nazis have purchased 27 properties this year, and 22 last year.²⁵ Across Germany, 'right-wing extremists own 146 properties', though other observers believe this figure to be too low.²⁶ In the US, a member of The Base reportedly purchased 30 acres of land in rural Washington state in 2018 with plans to use it as a training site.²⁷

In addition to using it as a training site, owning land provides radicalised individuals with the ability to meet more privately and avoid issues relating to permits for public marches or with private venues refusing them service. The acquisition of sufficient land, meanwhile, allows for the formation of outposts of radicalised individuals, with the land trading hands between likeminded individuals. An attempt at this occurred in 2014 in the small town of Leith in North Dakota, where a group of neo-Nazis purchased

19. Nicholas K Geranios, 'Aryan Nations Founder Moves', *ABC News*, 7 January 2006.

20. Southern Poverty Law Center, 'Case Docket', <<https://www.splcenter.org/seeking-justice/case-docket>>, accessed 12 November 2020.

21. For example, see David Smith, 'After Charlottesville: How a Slew of Lawsuits Pin Down the Far Right', *The Guardian*, 29 May 2018.

22. Mara Bierbach and Karsten Kaminski, 'Germany's Confusing Rules on Swastikas and Nazi Symbols', *DW*, 14 August 2018.

23. Bruce Hoffman and Jacob Ware, 'Is 3-D Printing the Future of Terrorism?', *Wall Street Journal*, 25 October 2019.

24. American Odyssey, 'Feuerkrieg Division Member Talks About New Group on Far-Right Podcast', 8 January 2019, <<https://medium.com/americanodyssey/feuerkrieg-division-member-talks-about-group-on-far-right-neo-nazi-podcast-314086068acf>>, accessed 17 November 2020; *Panorama*, 'Hunting the Neo-Nazis', 22 June 2020.

25. *DW*, 'Germany: Eastern States Ally Against Neo-Nazi Property Deals', 28 September 2020.

26. David Crossland, 'German Far-Right Buys Land for Military Training', *The Times*, 30 July 2020; MOBIT, 'Nach den rechten Häusern sehen', December 2017, <https://mobit.org/Material/MOBIT_Nach%20den%20rechten%20Häusern%20sehen_2018.pdf>, accessed 12 November 2020.

27. Chad Sokol, 'Report: Leader of Neo-Nazi Terrorist Group Owns Land in Ferry County', *Spokesman-Review*, 23 January 2020, <<https://www.spokesman.com/stories/2020/jan/23/report-leader-of-neo-nazi-terrorist-group-owns-land/>>, accessed 12 November 2020.

multiple parcels of land and moved in several families in an attempt ‘to turn Leith in to a white supremacist enclave’.²⁸ The purchase of land allows violent extremists to congregate freely, exchange ideas and plan. For example, the Aryan Nations used an Idaho compound as a meeting space which hundreds of individuals visited and where several violent terrorists met and plotted.²⁹

Counterterrorism Financing Policies and Their Impact

There has been a push in the last five years by mainstream financial services to restrict or bar extremists from using their banking services, and social media sites have worked to demonetise content produced by designated radical actors.³⁰ This certainly helped reduce the revenue of several extremist groups and actors. However, the corresponding expansion of cryptocurrency has meant that there are still methods through which these groups can finance and spend, and such transactions are generally untraceable.³¹ For example, the Nordic Resistance Movement has received more than 1 million Swedish krona (around £88,000) in cryptocurrency from anonymous donors.³² This must now be part of the thinking of investigators, and public sector groups and think tanks need to consider innovative ways to monitor the crypto capabilities of these groups and individuals. It should also be noted that while cryptocurrencies are difficult to trace, it is not impossible. For example, looking at transactions using common numerology in extremist circles can provide information on groups, while converting currency like Bitcoin into a more traditional format can leave a paper trail.³³ Still, other extremists have struggled to acquire or navigate new technology, preferring more traditional avenues, meaning observers cannot overlook ‘old-school’ methods.

In the case of lone actors in particular, attempting to monitor purchases of certain items will not always prove sufficient to prevent a terrorist attack. Red flag purchases of chemicals used to build bombs or of high-capacity firearms and ammunition may help law enforcement identify and foil certain plots, but terrorists need only rent a car, purchase a

knife, or acquire a firearm without a background check to be able to perpetrate mass violence. In some instances, following the money will only help retrace the steps of an attacker after the fact. This will be even more likely if 3D printing becomes more affordable and accessible. This should not deter *ex post facto* financial investigations, which can still unearth a web of connections between extremist networks and actors not known to law enforcement.

Conclusion

Already a challenging task, forecasting the future of right-wing extremist and terrorist financing is circumspect at best given the unpredictability that comes with a global pandemic. Just as the coronavirus pandemic has had significant negative impacts on state economies and the smooth operation of global finance, it has also disrupted right-wing terrorist financing. One likely outcome is a furthering of the trend away from group structures (now weakened by a lack of fundraising avenues) towards lone actor terrorism. Financial downturns will leave people more vulnerable to extremist narratives and lockdowns increase individual’s exposure to potential radicalisation online. This may translate into an increased number of extremists as well as terrorists. However, the pandemic likewise limits potential terrorists’ ability to fundraise through traditional formats and may, in some cases, leave them financially unable to mount an attack. The coronavirus pandemic has undoubtedly thrown right-wing extremism and terrorism off its path of steady, rapid growth. A rise in the number of radicalised individuals, paired with a decline in capital, means that the violent fringe of the right-wing may emerge from lockdown as something totally different from what observers have seen before.

Bethan Johnson is based at the University of Cambridge. She is the leader of the Political Violence and Terrorism Research Unit of the Centre for Analysis of the Radical Right, the leading information hub for the radical right. She is the series editor for the forthcoming *Analyzing Political Violence* book series published with ibidem Press/Columbia University Press.

28. Ryan Lenz, ‘Amid Worries of Nazi Sympathizers on the Town Council, Leith, North Dakota, Moves to Dissolve’, Southern Poverty Law Center, 21 June 2018, <<https://www.splcenter.org/hatewatch/2018/06/21/amid-worries-nazi-sympathizers-town-council-leith-north-dakota-moves-dissolve>>, accessed 12 November 2020.
29. Daniel J Wakin, ‘Richard G. Butler, 86, Founder of the Aryan Nations, Dies’, *New York Times*, 9 September 2004; Southern Poverty Law Center, ‘Aryan Nations’, <<https://www.splcenter.org/fighting-hate/extremist-files/group/aryan-nations>>, accessed 12 November 2020.
30. Examples of this include restrictions on advertised content on YouTube and Facebook, as well as bans or restrictions by GoFundMe, PayPal and Patreon.
31. Davis, ‘New Technologies But Old Methods in Terrorism Financing’, p. 2.
32. Magnus Ranstorp and Filip Ahlin (eds), ‘Executive Summary: From the Nordic Resistance Movement to the Alternative Right, a Study of the Swedish Radical Nationalist Milieu’, Swedish Defence University, p. 3.
33. Gerard, ‘Neo-Nazis Bet Big on Bitcoin (and Lost)’.