Project craaft

Collaboration, Research & Analysis Against the Financing of Terrorism

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

New Technologies but Old Methods in Terrorism Financing

Jessica Davis

Research Briefing No. 2

About Project CRAAFT

Project CRAAFT is an academic research and community-building initiative designed to build stronger, more coordinated counterterrorist financing capacity across the EU and in its neighbourhood. Project CRAAFT is funded by the 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 projectcraaft.eu.

This publication was funded by the European Union's Internal Security Fund — Police. The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

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

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 cryptocrrency 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 Isil', *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 though 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.