2023

Financing Violent Extremism: An Examination of Maligned Creativity in the Use of Financial Technologies

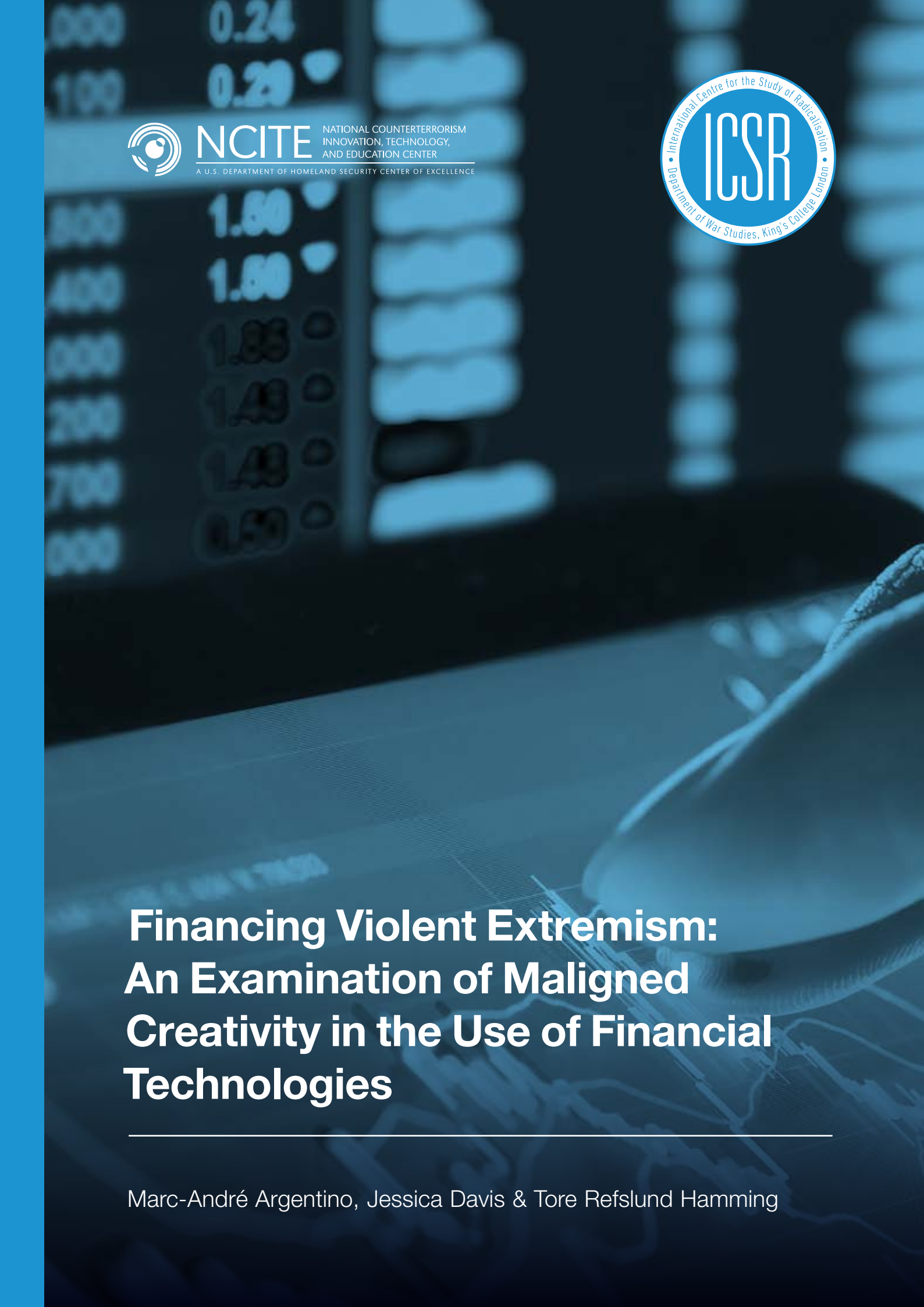
Marc-Andre Argentino
King's College London

Jessica Davis
King's College London

Tore Refslund Hamming
King's College London

National Counterterrorism Innovation, Technology, and Education Center

International Centre for the Study of Radicalisation



NCITE
NATIONAL COUNTERTERRORISM INNOVATION, TECHNOLOGY, AND EDUCATION CENTER
A U.S. DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

International Centre for the Study of Radicalisation
ICSR
Department of War Studies, King's College London

Financing Violent Extremism: An Examination of Maligned Creativity in the Use of Financial Technologies

Marc-André Argentino, Jessica Davis & Tore Refslund Hamming

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 20STTPC00001-01-00. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. +44 20 7848 2098
E. mail@icsr.info

Twitter: @icsr_centre

Like all other ICSR publications, this report can be downloaded free of charge from the ICSR website at **www.icsr.info**.

Executive Summary

This workbook teaches researchers, analysts and practitioners how different sorts of terrorist and violent extremist actors utilise financial technologies and cryptocurrencies to finance their operations. The process of terrorist adoption of financial technologies is spelled out for various organisations and can assist analysts to estimate whether and when a group or terrorist actor would embrace a financial technology or cryptocurrency. The workbook also includes terms that may be used to search information holdings for terrorist adoption of cryptocurrencies or financial technologies, offering early warning of terrorist adoption.

- Most terrorist organisations, cells and individuals gradually embrace new technology, tactics, strategies and processes. Finance is more confined by external constraints than other areas of potential innovation and adaptation, hence few organisations or entities actually innovate in finance.

- Most terrorist actors are bound by financial and economic institutions, making terrorist financing difficult to innovate. Structures control them. Thus, terrorist finance patterns and approaches are better regarded as adaptation and learning rather than innovation.

- When economic and financial systems evolve, most terrorists adapt to new financing methods. Terrorists employ financial technologies and cryptocurrencies when they are convenient and widely used. Until then, motivated individuals or cells can innovate, but groups or more established cells or organisations seldom adopt new financing methods early.

Table of Contents

1. Introduction

The purpose of this workbook is to examine terrorist financial adaptation, particularly in the context of new financial technologies (fintech) and cryptocurrencies. We begin by explaining our methods and data collection and defining key terms, and then explore different types of terrorist financial adaptation and innovation. We then consider how these financial mechanisms can be best countered in the context of the global fight against terrorist financing and conclude with a discussion on detecting terrorist adaptation in the financial space.

In this workbook, there is a significant focus on cryptocurrency, in part because it is new. However, while some space has to be dedicated to explaining and describing cryptocurrencies, other financial technologies appear to play an equal if not greater role in facilitating terrorist financing.

Cryptocurrency, a financial technology in itself, is a decentralised payment and monetary system that uses internet architecture and is built on blockchain technology (see key terms, below). While it has been designed as an alternative monetary system, in practice it functions primarily as a method of sending value or processing payments, with users ultimately purchasing coins using state-backed currency and selling cryptocurrency to purchase state-backed currency, which is more easily used for everyday purchases and activities. Cryptocurrencies can also be seen as assets: some people purchase cryptocurrency coins and hold them as investments, since their value fluctuates.[1] While some have a difficult time conceptualising cryptocurrency as "money", since it is not backed or created by a state, it can be helpful to remember that even state-backed money operates on a system of belief and trust: that the currency a user holds will be accepted by other users for an agreed price. Modern state-backed currencies have no intrinsic value and are not representative of other assets (like gold); cryptocurrencies are simply an extension of this. Proponents of cryptocurrency suggest that they offer greater privacy, independence and functionality than state-backed currencies, while detractors suggest that few of these promises have been realised. Functionally, approximately 20% of people in the United States own bitcoin, one form of cryptocurrency,[2] though globally the percentage of a population is likely to vary significantly depending on the technological adoption of a particular jurisdiction. Cryptocurrencies are now widely seen as part of the modern global monetary system and are used by illicit actors, including terrorists, to finance their activities.

1 Coinbase, "What Is Cryptocurrency?," accessed 21 November 2022, https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency.
2 Alex Lielacher, "How Many People Own & Use Bitcoin in 2022?," accessed 21 November 2022, https://cryptonews.com/exclusives/how-many-people-own-use-bitcoin-2022.htm.

2. Method and Data Collection

For this project, we were faced with a challenge of scope and scale in terms of analysing how official and non-official threat actors are or are not using cryptocurrencies for their extremist or terrorist activities. The researchers focused on groups or actors that have been proscribed by Five Eyes governments to limit the scope of research. For jihadist actors, the focus was on the larger umbrella organisations rather than affiliates. For racially or ethnically motivated violent extremism (REMVE) and anti-government, anti-authority violent extremism (AGAAVE) actors, we included an additional section on the use of cryptocurrencies by post-organisational violent extremist and terrorist groups. In the REMVE and AGAAVE space, the landscape is shifting away from group structures (potentially, in part, as an adaptation to counter-terrorist financing policies and practices) and in some cases away from the formal financial sector entirely, so it is important also to consider how cryptocurrencies are used and perceived by this growing loose transnational network of threat actors.

The main source of data we used is the internal ICSR archive of material relating to violent extremist and terrorist actors that the centre has been collecting for well over a decade. As ICSR is a well-established and prominent academic research centre, we therefore possess a formidable archive of relevant material. Moreover, our institutional process of data collection is ongoing, meaning this archive is continuously updated with new material. The archive include smaterial from a variety of threat actors across the politically motivated, religiously motivated and ideologically motivated spectrum of violent extremists.

The material sourced from the database for this project stems from REMVE, AGAAVE and jihadist owned and operated websites and/or forums: Telegram channels and chats, Rocket.Chat, Wire, TamTam, VK, Gab, MeWe, WimKin, Parler, Gettr, Rumble, Bitchute, LBRY, Minds Element, 4Chan, 8kun, Onion-based websites and Odysee.

3. Key Terms

Adaptation
Adaptation is the process of adjusting existing methods and techniques by terrorist or extremist organisations or operational actors.[3]

Altcoin
Any currency that is not bitcoin is referred to as an altcoin. Altcoins range from the second-most popular currency, Ethereum, to hundreds of distinct coins with relatively little market share.

Block
Data sets inside a blockchain. In the context of a cryptocurrency blockchain, blocks are made up of transaction records created when users purchase or sell currencies. Each block can only carry a certain amount of data. When it reaches this limit, a new block is created to continue the chain.

Blockchain
A digital way of keeping track of things; the technology that makes cryptocurrencies work. A blockchain is a list of transactions that is permanent and cannot be changed. It is made up of blocks that are added one after the other.

Chain-Hopping
Chain-hopping is the process of moving from one cryptocurrency blockchain to another. This is common when purchasing the privacy coin Monero but can also be done with other coins. It is most often performed in an effort to break a financial trail and make it more difficult for investigators to follow the source or destination of funds.

Clustering
Clustering is a de-anonymisation approach for blockchain data. It connects many wallets belonging to the same person or business.

Cold Wallet / Cold Storage / Hard Wallet
A way to store your cryptocurrency outside the internet. Many cold wallets are devices that look like USB drives. This kind of wallet can help to keep your cryptocurrency safe from hackers and thieves, but it also comes with its own risks, such as misplacing it (and with it, your cryptocurrency).

Exchange
A cryptocurrency exchange is an online market where you can buy and sell cryptocurrency.

3 Adam Dolnik, *Understanding Terrorist Innovation: Technology, Tactics and Global Trends*, 1st edition (Routledge, 2007).

Fork
When the users of a blockchain modify its rules. Changes to a blockchain's protocol often result in two new paths: one that follows the existing regulations and another that branches off from the previous rules.

Hash
A distinct string of numbers and letters that identifies blocks and is linked to cryptocurrency buyers and sellers.

Hawala
Hawala is an informal value transfer system used to move money around the world. It is particularly popular in non-Western countries. Hawala transactions involve the movement of money between two locations without the physical transfer of funds, either domestically or internationally. Instead of moving money physically, a *hawaladar* will contact a business associate and ask for the funds to be released to the intended beneficiary. Later, entirely independently of the original transaction (and only if or when an imbalance occurs between the two businesses), the two *hawaladars* will settle their accounts through a fund transfer (potentially through a money service business or bank) or perhaps through goods or services.

Hot Wallet
A bitcoin wallet that is software-based and linked to the internet. While hot wallets are more convenient for immediately accessing your cryptocurrency, they are more vulnerable to hacking and cybersecurity threats than offline 'cold' or 'hard' wallets.

Innovation
Terrorist innovation is the introduction of a new method, technique or technology not adopted by any other terrorist organisation in the past.[4] This includes both tactical and technological innovation, as well as strategic and organisational innovation.[5]

Mixers
Mixers, also known as mixing services, are platforms that seek to conceal the source and destination of cryptocurrency transactions. The goal is to make transactions untraceable and anonymous. To do this, the mixer will combine coins and transfer them to several wallet addresses. Mixers are employed by certain users to conceal huge transactions and to escape hackers. Mixers can also be used by criminals to launder the proceeds of illegal activity. As a result, they pose a concern in terms of money laundering and terrorist financing.

Non-Fungible Tokens (NFTs)
Non-fungible tokens are value units used to represent ownership of one-of-a-kind digital assets, such as art or collectibles. NFTs are often stored on the Ethereum blockchain.

4 Dolnik.
5 Mauro Lubrano, "Navigating Terrorist Innovation: A Proposal for a Conceptual Framework on How Terrorists Innovate," *Terrorism and Political Violence*, 5 April 2021, 1–16, https://doi.org/10.1080/09546553.2021.1903440.

Privacy coin
A privacy coin, also called an anonymity-enhanced coin, is difficult to track on the blockchain and increases the privacy and anonymity of its users through transactional features. It lets the user conduct transactions without revealing the amount, source and destination of funds, thus making it difficult to trace on the blockchain. Monero is the most commonly known privacy coin but others are in circulation, such as Dash, Zcash and Grin. Due to their privacy features, privacy coins have a higher risk of being associated with financial crime than other cryptocurrencies.

Public Key
The address of your wallet, which is similar to your bank account number. You can provide individuals or institutions your public wallet key so that they can send you money.

Private Key
The encryption code that enables you to access your cryptocurrency directly. Your private key, like your bank account password, should never be shared.

Recovery Phrase / Seed Phrase
A recovery phrase unlocks your wallet. Anyone with the recovery phrase can gain access to the cryptocurrency in your wallet. Often referred to as the key, it makes up part of the idiom “not your keys, not your coins”. Whoever controls the key or has the recovery phrase controls the coins. This is a human-readable version of the private key.

Wallet
A location to keep your cryptocurrency assets. Digital wallets are available on several exchanges. Wallets may be ‘hot’ (internet, software-based) or ‘cold’ (physical, offline, usually on a device).

4. Financial Innovation in the Jihadist Space

In contrast with the general fear that jihadists will employ innovative fintech methods to fund their activities, there remains little empirical evidence supporting the assertion that jihadists have in fact embraced innovative technological solutions to secure and transfer funds in a widespread manner. Jihadist organisations generally rely on a diversification strategy in terms of their sources of financing to maximise their income and make it less vulnerable to detection and seizure. These sources include the sale of illicit goods (including drugs), donations, ransom payments, theft and, most importantly, territorial control, which enables extensive taxation.[6] None of al-Qaeda, the Taliban or Islamic State appear to have employed cryptocurrency extensively, while some groups, such as Hamas, have shown more interest in new financing technologies. The financial innovation by jihadists, particularly as it relates to cryptocurrency and fintech, is largely piecemeal, more "proof of concept" than a widespread change in techniques. In some cases, individuals and small cells have used financial technologies such as PayPal and online marketplaces, including eBay and Amazon, to procure weapons and components for attacks.[7] In the majority of cases, jihadists are employing similar methods to raise, use, move, store, manage and obscure funds, but have adopted fintech to do so. This is more reflective of economic and financial system changes than terrorist financial innovation.[8] However, as financial technologies continue to permeate economic and financial systems globally, jihadists are likely to adopt these technologies to facilitate their financial transactions.

Al-Qaeda

Over the course of its more than thirty years of existence, al-Qaeda has evolved from a small contingent of fighters based in the Afghanistan-Pakistan region to a global enterprise with formal affiliates in a range of countries in addition to numerous supporting networks. Besides its international terrorist activities, the global al-Qaeda network is involved in several active insurgencies in the Middle East and Africa as part of the group's endeavour to establish religio-political entities in the form of local emirates or, ultimately, a caliphate.

To fund its various activities, al-Qaeda has used a wide variety of financing methods. These have evolved with technological changes in society. For example, the group's fundraising methods have included a variety of activities, such as credit card theft,[9] bank robberies,

6 Andrew Mines and Devorah Margolin, "Cryptocurrency and the Dismantling of Terrorism Financing Campaigns," Lawfare Blog, 26 August 2020.
7 Jessica Davis, "How Terrorists Use the Internet for Weapons and Component Procurement," GNET (blog), 26 February 2020, https://gnet-research.org/2020/02/26/how-terrorists-use-the-internet-for-weapons-and-component-procurement/.
8 Jessica Davis, "New Technologies but Old Methods in Terrorism Financing," Royal United Services Institute for Defence and Security Studies, CRAAFT Research Briefing, no. 2 (22 July 2020): 7.
9 Colin P. Clarke, *Terrorism, Inc.: The Financing of Terrorism, Insurgency, and Irregular Warfare* (Santa Barbara, CA: Praeger, 2015): 139.

burglaries and forging cheques.[10] Early on, al-Qaeda primarily relied on donations from wealthy individuals, including its late founder Osama bin Laden, and funds diverted from companies and charities.[11] In more recent years, the group has reduced its reliance on centralised financing mechanisms, a response potentially prompted by counterterrorism financing pressures. Instead, it encourages affiliate groups and operational cells to finance their own activities.[12] In some cases, the core al-Qaeda group has even relied on its franchises to send money back to the leadership.[13] For example, in 2005, al-Qaeda's second in command at the time, Ayman al-Zawahiri, reached out to the head of al-Qaeda in Iraq to request $100,000 as financial assistance.[14]

To move money, the group has relied on a variety of means, including *hawala*, the formal financial sector and non-governmental or charitable organisations, as well as front companies. Cash couriers were also a popular method of moving funds for the group, particularly prior to the terrorist attacks of 11 September 2001.[15]

Al-Qaeda has never issued an official statement on the legality of cryptocurrency or any instructions for how to use it. In fact, if one searches al-Qaeda's Rocket.Chat 'GNEWS server' for 'cryptocurrency', 'bitcoin', 'btc', 'monero' and 'wallet', no results emerge. However, in March 2019, Syria-based jihadist ideologue Abdallah al-Muhaysini, who used to be close to al-Qaeda, published a video endorsing bitcoin and calling on jihadists to donate to Hamas.[16]

There are a handful of examples of al-Qaeda platforms and operational cells soliciting cryptocurrency donations. Likewise, some adherents have solicited funds using social media platforms, in particular the encrypted platform Telegram.[17] For instance, in 2017, the al-Sadaqah website, run by an al-Qaeda-linked network, used Facebook and Telegram to solicit donations from its supporters in bitcoin.[18] In February 2018, the "tech talk" section of a pro-al-Qaeda English-language magazine, *al-Haqiqa*, examined the permissibility of using bitcoin and other cryptocurrencies to fund al-Qaeda activities.[19] Another campaign was launched by Syria-based al-Qaeda and affiliated terrorist groups using Telegram channels and other social media to solicit cryptocurrency donations under the guise of charity.[20] The extensive reliance on charitable causes highlights a financing method that militant Islamists have employed for years.

Al-Qaeda currently has leadership figures in both Afghanistan and Iran. To date, the Afghan economy has minimal cryptocurrency integration. There are some reports of humanitarian aid being sent to the

10 Kevin McGrath, *Confronting Al-Qaeda: New Strategies to Combat Terrorism* (Naval Institute Press, 2011): 75.
11 Jodi Vittori, *Terrorist Financing and Resourcing*, 2011 edition (New York, NY: Palgrave Macmillan, 2011): 39.
12 Jessica Davis, *Illicit Money: Financing Terrorism in the 21st Century* (Boulder, CO: Lynne Rienner Publishers, 2021).
13 McGrath, *Confronting Al-Qaeda*: 75.
14 Clarke, *Terrorism, Inc.*: 134.
15 McGrath, *Confronting Al-Qaeda*: 78.
16 Steven Stalinsky, "Fears About New Facebook Cryptocurrency Are Overblown – While Main Threat Of Criminal Activity On Telegram App Is Being Criminally Ignored," MEMRI, 16 July 2019.
17 "United States of America v. 155 Virtual Currency Assets," United States District Court for the District of Columbia, 13 August 2020.
18 Nikita Malik, "How Criminals And Terrorists Use Cryptocurrency: And How To Stop It," *Forbes*, 31 August 2018, sec. Cybersecurity, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/.
19 Ahmad Helmi Bin Mohamad Hasbi, "Cryptocurrencies: Potential for Terror Financing?" 23 May 2018, https://isnblog.ethz.ch/technology/cryptocurrencies-potential-for-terror-financing.
20 Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns" (Department of Justice, 13 August 2020), https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

country through cryptocurrency,[21] but wider use remains minimal.[22] As such, al-Qaeda in Afghanistan plausibly finances itself in much the same way that other groups and actors in the country do: through taxation and extortion (if and when this is available to them, based on territorial control and influence), support from the Taliban or other groups, some donations from support networks and through criminal activity.[23] A more likely use of cryptocurrency by al-Qaeda exists for the leadership in Iran, given the country's use of cryptocurrencies for sanctions evasion.[24] However, to date, there is little indication that cryptocurrency funds are financing the al-Qaeda leadership in Iran.

With its affiliates self-financing primarily through their territorial control or local activities and a core group with few economic needs, the group has little incentive to innovate in terms of financial strategy. Furthermore, the group has relatively well-developed fund-movement mechanisms, such as cash couriers and formal banking channels, that it can use to move funds between operational theatres as required. To date, there is little indication that al-Qaeda is interested in adopting cryptocurrencies or fintech as means of moving funds.

Taliban

The Taliban has its origins in the early 1990s in Afghanistan, where it first emerged as a local militia but in just a few years grew strong enough to take control of the entire country, which it governed for a five-year period before being ousted. First as a state power and later as a nation-wide but strongly embedded insurgency, the Taliban has been raising funds from a variety of different activities and these have only been solidified with its takeover of Afghanistan in 2021. The group's funding mechanisms can be broadly categorised as taxation and extortion activities, state sponsorship, donations from wealthy individuals, kidnapping for ransom and the drug trade. However, within Afghanistan, there is diversity in terms of how different Taliban factions raise funds.[25] In some regions, a group will focus on taxing border crossings,[26] while in others members tax natural and farmed resources.[27] Increasingly, the group is also believed to be profiting from aid shipments.[28]

While the Taliban has many sources of income, it also has considerable costs, particularly now that it is responsible for administering the economic and financial systems in Afghanistan. Its recent budget indicated a shortfall of nearly $500 million, with no plan to bridge the gap between planned expenditures and revenues.[29] The group uses primarily Afghanistan-based mechanisms to move, store and manage

21 David Z. Morris, "Bitcoin Won't Save the Afghan People," CoinDesk (blog), 3 September 2021, https://www.coindesk.com/tech/2021/09/03/bitcoin-wont-save-the-afghan-people/.
22 Alex Zerden, *Are Terrorist Groups Using Cryptocurrency in Afghanistan?* CoinDesk (blog), 1 October 2021, https://www.coindesk.com/video/community-crypto-on-cdtv-clips/are-terrorist-groups-using-cryptocurrency-in-afghanistan.
23 Jessica Davis, "Illicit Financing in Afghanistan: Methods, Mechanisms, and Threat-Agnostic Disruption Opportunities," SOC ACE Research Paper (University of Birmingham, May 2022).
24 Tom Robinson, "How Iran Uses Bitcoin Mining to Evade Sanctions," 21 May 2021, https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions.
25 Jessica Davis, "The Challenges of Understanding Taliban Finance," Lawfare (blog), 23 August 2021, https://www.lawfareblog.com/challenges-understanding-taliban-finance.
26 Yaroslav Trofimov, "Taliban Find New Revenues as They Seize Afghanistan's U.S.-Built Border Gateway," *Wall Street Journal*, 5 July 2022, https://www.wsj.com/articles/taliban-find-new-revenues-as-they-seize-afghanistans-u-s-built-border-gateway-11625495521?st=b5m9feropl929nz&reflink=desktopwebshare_twitter.
27 David Brennan, "Nut Jihad: Taliban Makes Millions From Pistachio Farms," *Newsweek*, 26 March 2018, https://www.newsweek.com/funding-terror-snacks-taliban-rake-millions-pistachio-profits-860393.
28 Abubakar Siddique, "Afghans Accuse The Taliban Of Misappropriating Foreign Aid," *RFE/RL*, 27 October 2021, sec. Afghanistan, https://gandhara.rferl.org/a/afghanistan-taliban-foreign-aid-misappropriation/31532541.html.
29 Ayaz Gul, "Taliban Announce First Annual Afghan Budget," *VOA*, 14 May 2022, https://www.voanews.com/a/taliban-announce-first-annual-afghan-budget-/6573685.html.

funds, relying significantly on cash couriers, the *hawala* system in Afghanistan and, to a lesser extent, the formal banking system, particularly correspondent banking relationships in the region.[30]

Over the course of the last twenty years, the Taliban has demonstrated little in the way of adaptation or innovation in terms of its financing. In part, this is due to a lack of pressure to change the way it does things: the international community's ability to disrupt Taliban finance has been limited and is even more so now that the group controls the entirety of Afghanistan (for all intents and purposes, despite some ongoing disputes). The group's control of Afghanistan and the international response to that has resulted in a humanitarian and economic crisis, but Taliban finances are relatively resilient to counterterrorism efforts due to its ability to control territory and the lucrative nature of the drug trade.

As with al-Qaeda and the Islamic State cell in Afghanistan, the Taliban could conceivably use the emerging nexus between cryptocurrency and *hawala* in the country to conduct transactions. (See the section on Hamas for a description of this nexus and its importance.) However, the Taliban has little incentive to adopt cryptocurrencies, as its existing financing mechanisms serve it well. It already has in place a system of money transfer, obfuscation techniques (including potentially with the help of professional enablers) and freedom of movement in Afghanistan.[31]

Islamic State

Originally growing out of al-Qaeda's Iraqi affiliate headed by Abu Musab al-Zarqawi, Islamic State (IS) officially split from the global al-Qaeda network in early 2013. Now acting as an independent group, it quickly established itself in the Syrian civil war insurgency before declaring its caliphate in June 2014, which facilitated further geographical expansion outside the Levant region through its province structure. Between 2014 and 2019 it succeeded in controlling large swathes of territory in Syria and Iraq that gave rise to the implementation of a proto-state entity governed by its interpretation of sharia law. Running a state-like entity and controlling numerous provinces around the world, IS was dependent on a large influx of funding but also able to tap into vast opportunities to diversity its funding channels.

As is the case for al-Qaeda, IS does not officially promote the use of cryptocurrency in its propaganda and there is limited information confirming whether the group formally uses any sort of cryptocurrency or has adopted fintech widely. Instead, the core group makes use of the financial system in its areas of operations in order to finance its activities. This primarily means a reliance on money service businesses, cash and the formal banking system when and if available. On numerous occasions, however, IS's supporter networks and sympathetic individuals have promoted the use of cryptocurrencies and in some cases have invested in currencies – mainly bitcoin – to fund various types of activities.[32]

30 Davis, "Illicit Financing in Afghanistan".
31 Davis, "Illicit Financing in Afghanistan".
32 John Templon, Anthony Cormier and Jason Leopold, "Secret Documents Show How Terrorist Supporters Use Bitcoin – And How The Government Is Scrambling To Stop Them," BuzzFeed, 8 February 2021.

For example, the supporter network I'lam Foundation has solicited cryptocurrency donations to fund its activities, which include translations of IS propaganda. The publicly available information for the process of donating is kept to a minimum and supporters are instructed to contact a Telegram channel to obtain the wallet address.[33] This form of financial tradecraft prevents attribution of the wallet address to terrorist activities, allowing the wallet to remain private and stopping blockchain-analytics companies and intelligence services from determining how much money is being sent to the wallet unless they are able to infiltrate the Telegram group and obtain the address.

IS sympathisers are not entirely supportive of the use of cryptocurrencies. The well-known supporter network Electronic Horizons Foundation has on occasion warned against the use of bitcoin due to the risk of authorities tracing the payments. Other networks entirely abandoned bitcoin and instead began using the privacy coin Monero.[34]

Several times, however, Western-based IS sympathisers have used cryptocurrencies to transfer funds to the group,[35] in addition to providing guidance on how to use cryptocurrencies, as illustrated by the case of Ali Shukri Amin.[36] In some cases, IS supporters have used cryptocurrencies to provide funds to individuals in detention facilities in Syria in an effort to help them to escape or to provide them with money for sustenance.[37],[38] These "pop-up" financial networks contribute to instability in the camps by facilitating a network that moves supplies, money and family members in and out of the camps.[39] However, cryptocurrency transactions are not the most popular method of moving funds into Syria.[40]

IS's adoption of cryptocurrency is probably based on the specific skillsets of individuals involved. To date, there is no overarching effort by the group or its affiliates to move their financial activities to cryptocurrency or other fintech. However, individual supporters have used and will continue to use new fintech to move funds for the group. To a certain extent this adoption mirrors the broader societal trends of adopting these new technologies, rather than a specific effort on the part of IS to innovate how it manages the movement of funds. As such countries as the Democratic Republic of the Congo seek to incorporate cryptocurrency and fintech more concretely into their financial systems, this is likely to create opportunities for IS operating in these areas to incorporate this financing method into the mechanisms it currently uses.

33 Laith Alkhouri and Lucas Webber, "I'lam Foundation for Translations Emerges as a Boon to Pro-Islamic State Media Ecosystem," Militant Wire, 18 April 2022.
34 Bridget Johnson, "ISIS Cyber Group Warns of Tracking Through Bitcoin Use," HS Today, 20 April 2021.
35 Daniel Palmer, "US Woman Gets 13 Years in Jail After Funding ISIS With Cryptocurrency," CoinDesk, 16 March 2020.
36 United States Department of Justice, "Manassas Man Pleads Guilty to Providing Material Support to ISIL," 11 June 2015.
37 Lizzie Dearden, "British Isis member who used Bitcoin to free jihadis from Syrian prisons jailed for 12 years," *The Independent*, 3 September 2021.
38 Duncan Gardham, "Hisham Chaudhary: Bitcoin Jihadist Jailed for 12 Years after Sending £55,000 to Islamic State," *Sky News*, 3 September 2021, https://news.sky.com/story/hisham-chaudhary-bitcoin-jihadist-jailed-for-12-years-after-sending-55-000-to-islamic-state-12398528.
39 Audrey Alexander, "'Help for Sisters': A Look at Crowdfunding Campaigns with Potential Links to Terrorist and Criminal Networks," GNET (blog), 22 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/.
40 Audrey Alexander and Teddy Macdonald, "Examining Digital Currency Usage by Terrorists in Syria," *Combating Terrorism Center at West Point* 15, no. 3 (31 March 2022), https://ctc.westpoint.edu/examining-digital-currency-usage-by-terrorists-in-syria/.

Hamas

Unlike al-Qaeda and IS, but similar to the Taliban, Hamas is a political movement and nationalist Islamist group employing violence to realise its political objective of establishing an Islamic Palestinian state. A designated terrorist group and affiliated with the Muslim Brotherhood movement, Hamas is primarily active in Gaza, where it is the dominant political authority, and, to a lesser extent, on the West Bank.

With its long history, social embeddedness and political control, Hamas uses multiple methods to fund its activities and has a relatively sophisticated financing structure. Despite being a Sunni fundamentalist group, it receives significant state funding from Iran, usually in the tens of millions of dollars annually.[41] It has also used the charitable sector to raise and move funds,[42] establishing a website in 2002 to solicit donations specifically for the purchase of weapons. These donations were transferred through the banking system to accounts held in Gaza.[43] Hamas also raises and moves funds through trade-based money-laundering schemes, some of which include transit across Turkey.[44]

In recent years, Hamas has solicited cryptocurrency donations globally and used social media to draw attention to its request for donations. The group used financial tradecraft in an attempt to make the bitcoin donations it receives truly anonymous, such as through the creation of unique bitcoin addresses for each individual donor.[45] Israel has disrupted multiple Hamas financing operations using cryptocurrency, including exchanges operating in the West Bank and Gaza.[46] Despite these disruptions, Hamas will likely continue to use cryptocurrency to finance its activities and will try to innovate techniques to obscure the source and destination of funds using cryptocurrencies; such techniques could be exported to other jihadist groups.

Hamas operates one of the more financially innovative financing strategies in the militant Islamist space. The group has solicited donations, made attempts at generating anonymous donations and wallets, and controls or significantly influences cryptocurrency exchanges in or near its areas of operations. To remove funds from the cryptocurrency exchanges, Hamas makes use of either official exchanges, converting that money into cash, or uses informal exchanges. (Informal exchanges are essentially *hawalas* or money service businesses that also have cryptocurrency capabilities, meaning that individuals can transfer funds in cryptocurrency to the *hawala* or business address, then "cash out" into their desired form of currency.) Despite the relatively widespread use of cryptocurrency and other financial technologies in Israel and the Palestinian territories, Hamas still needs to convert cryptocurrency into cash in order to use funds. Hamas' financial innovation is being carried out within

41 Vittori, *Terrorist Financing and Resourcing*: 73; Anna Ahronheim, "Iran Pays $830 Million to Hezbollah," *Jerusalem Post*, 15 September 2017, https://www.jpost.com/Middle-East/Iran-News/Iran-pays-830-million-to-Hezbollah-505166.

42 Matthew Levitt, *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*, 1st edition (New Haven, CT: Yale University Press, 2007).

43 Vittori, *Terrorist Financing and Resourcing*: 61.

44 Anna Ahronheim, "Israeli Spy Agency Uncovers Gaza-Turkey-West Bank Terror Money Trail," *The Jerusalem Post*, 6 August 2017, https://www.jpost.com/arab-israeli-conflict/israeli-spy-agency-uncovers-gaza-turkey-west-bank-money-trail-501506.

45 Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," 13 August 2020, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

46 Ahmad Abu Amer, "Hamas Plans to Continue Using Cryptocurrencies for Operations," Al-Monitor, 7 January 2022, https://www.al-monitor.com/originals/2022/01/hamas-plans-continue-using-cryptocurrencies-operations.

the context of broader cryptocurrency adoption in the Palestinian territories and Israel and is plausibly a function of that adoption rather than a specific strategy created by Hamas to finance its activities in this way. Indeed, cryptocurrency adoption is relatively high in the Palestinian territories: remittances account for the majority of cryptocurrency transactions into the territories, along with freelance payments, potentially a response to the restriction of other financial services into the area.[47]

47 Leigh Cuen, "In Palestine, Civilians Are Using Bitcoin More Than Hamas," CoinDesk, 22 August 2019, sec. Markets, https://www.coindesk.com/markets/2019/08/22/in-palestine-civilians-are-using-bitcoin-more-than-hamas/.

5. Financial Innovation in the REMVE and AGAAVE Space

Compared to jihadist groups, many racially and ethnically motivated violent extremism (REMVE) and anti-government, anti-authority violent extremism (AGAAVE) actors have adopted a more deliberate approach to cryptocurrency and fintech to finance their activities. In some cases, this is driven by ideology: the use of a non-state-backed currency has appeal for individuals or movements seeking to bring about the collapse of the Western financial system or simply to distance themselves from the state and its institutions. Many of these actors have also been drawn to the alleged anonymity of cryptocurrencies, although in recent years that anonymity has been demonstrated to be more pseudonymous than fully anonymous.

The main innovation in this space is the eschewing of formal group structures, which has further effects on these groups' adoption of fintech. The decentralised cell structure is potentially an adaptation to counterterrorist tools and techniques, including those associated with counterterrorism approaches to financing. These decentralised structures or even more nebulous movements have little in the way of financial needs, meaning that disrupting their financing has far less meaningful impact than it does for jihadist groups.

Furthermore, the individuals associated with these types of extremism often use a self-funding strategy, rarely reaching out to a broader movement or other individuals for help financing their activities. They tend to use tools and equipment readily available to them to conduct their attacks – another indication of potential adaptation to counterterrorism measures. Any movement- or organisational-level financing that occurs in support of specific actors tends to be after the fact, focusing on legal support.

At the movement level, extremist influencers and propagandists tend to use funds to cover costs and contribute to disseminating their propaganda. In some cases, individual propagandists and influencers profit from sharing or creating extremist content.

Atomwaffen Division / National Socialist Order

Atomwaffen Division (AWD), also known as National Socialist Order (NSO), is a terroristic neo-Nazi movement that arose from the Iron March internet forums. Members of the organisation tend to be accelerationists,[48] positing that violence is the only sure method to achieve their goals. The movement's primary ideological influences include James Mason, Charles Manson, Joseph Tommasi and

48 Members of AWD/NSO believe that modernity, liberalism and capitalism are inherently flawed and are the source of their own inevitable and accelerating demise. Accelerationists use a set of tactics and strategies designed to put pressure on and exacerbate latent social divisions, often through violence, thus hastening societal collapse. See: https://www.accresearch.org/shortanalysis/an-introduction-to-militant-accelerationism.

William Pierce. It relies on a decentralised cell structure,[49] which suggests that organisational financing for the overall movement is limited. The movement has associated cells in several countries, including Germany (Feuerkrieg Division),[50] the UK (Sonnenkrieg Division), Poland, Canada,[51] the Czech Republic and Ukraine.[52] AWD originally organised online, mostly through the communication platform Discord.[53] While there is no publicly available information suggesting that the group also raised money through Discord, the platform does provide the ability for users to generate funds through private servers, advertisements, donations and sponsorship. According to information submitted by the Government of Canada to the Financial Action Task Force, AWD's resources and financial structure are primarily based online, with reliance on money transfer services.[54]

Most of AWD/NSO funding reportedly comes from members' self-financing. For instance, AWD member William James Tschantre cashed in $3,000 of savings and quit his fast-food job before purchasing a pair of rifles and hundreds of rounds of ammunition.[55] The group might also use propaganda sales to support some aspects of the organisation and some of its members. For instance, AWD has used Amazon CreateSpace to sell propaganda,[56] selling merchandise that includes T-shirts, mugs and books. It then used some of these funds to support members accused of crimes but not to finance actual attacks.[57]

NSO and American Futurist, a propaganda website for AWD/NSO material, are now using NSvendor to sell related propaganda (specifically *Siege* by James Mason). American Futurist was set up in 2020 to spread propaganda. The site accepts donations through bitcoin and Monero and has instructions for sending physical currency to a post office box. American Futurist also has instructions on how to use Monero. These instructions first advise the purchase of a cryptocurrency like bitcoin using an exchange, such as CoinBase, followed by moving coins from the exchange to a private wallet, one hosted "on your computer that you're in control of". The instructions continue by recommending the user obtain a Monero wallet and exchange the coin for Monero using a wallet such as Exodus that allows for the transfer of cryptocurrencies without the use of an exchange. The article concludes with a description of cashing in Monero by exchanging it for another cryptocurrency, such as bitcoin, and then using an exchange or a bitcoin ATM. The website is effectively describing a method of chain-hopping and using Monero to obscure the source and destination of funds. While this method is technically correct, using a self-hosted wallet such as Exodus means

49 Jacob Ware, "Siege: The Atomwaffen Division and Rising Far-Right Terrorism in the United States," ICCT Policy Brief, 2019: 21.
50 Alexander Epp, "Neo-Nazi 'Atomwaffen Division' Spreads Fear in Germany," *Spiegel International*, 13 November 2019.
51 Mack Lamoureux and Ben Makuch, "Atomwaffen, an American Neo-Nazi Terror Group, Is in Canada," *Vice Canada*, accessed 16 October 2021, https://www.vice.com/en/article/a3a8ae/atomwaffen-an-american-neo-nazi-terror-group-is-in-canada.
52 Epp, "Neo-Nazi 'Atomwaffen Division'".
53 Jason Blazakis et al., "The Atomwaffen Division: The Evolution of the White Supremacy Threat," The Soufan Center, August 2020, https://thesoufancenter.org/wp-content/uploads/2020/08/The-Atomwaffen-Division-The-Evolution-of-the-White-Supremacy-Threat-August-2020-.pdf.
54 FATF, "Ethnically or Racially Motivated Terrorism Financing" (Paris, France, June 2021).
55 "Atomwaffen Division," Southern Poverty Law Center, accessed 16 October 2021, https://www.splcenter.org/fighting-hate/extremist-files/group/atomwaffen-division.
56 Davis, *Illicit Money*.
57 FATF, "Ethnically or Racially Motivated Terrorism Financing".

that the minimum amount of bitcoin that can be exchanged for Monero is roughly $150, a potential barrier to use for some donors.[58]

AWD/NSO uses funds for training camps, also known as "hate" camps, conducting weapons training and teaching combat skills. Attendees pool funds to acquire goods and weapons needed for the camp, essentially self-financing their training activities. The murders that AWD members have committed to date have been lone-actor, low-complexity attacks using weapons that the perpetrators already owned; while perpetrated by AWD members, it remains unclear whether all of the incidents were motivated by the group's ideology and carried out to advance its goals. Many of the members acquired their weapons and ammunition well in advance of any planned incident. For instance, one member was arrested with an AR15 and a thousand rounds of ammunition, a weapon he had possibly acquired some time before the incident.[59] In some cases, cells may have been preparing for more complex attacks. Following the arrest of AWD member Devon Arthurs, a cooler with HMTD was found by the police, as well as other explosive precursors and components including electric matches and empty ammunition casings with fuses, which can be used as detonators.[60]

Reports also suggest that members travel to visit international cells; in these cases, individual members have presumably paid for their own travel expenses. The group's accelerationist ideology, particularly its efforts to bring about the demise of the social order, suggests that it might be particularly inclined towards using alternatives to the formal financial system, such as cryptocurrencies, other fintech and gaming platforms with payment mechanisms. However, its organisational financing is limited and operational financing is likely largely self-funding. This in and of itself could demonstrate extremist adaptation and innovation in financing: the lack of organisational structure could be a deliberate innovation meant to complicate counterterrorism and counter-extremism responses to group-based organisation.

The Base

As with AWD/NSO, The Base's structure and strategies grew out of the demise of the Iron March internet forums. "Rather than fashioning itself as a distinct group, The Base from the beginning operated as a decentralised network of 'survivalism and self-defense' training camps. It also retained comms channels with many members in Atomwaffen Division."[61] The Base functions as a network of cells connected online.[62] Rinaldo Nazzaro, the founder and head of The Base, structured the organisation according to the "leaderless resistance" model pioneered by Louis Beam.[63] This organisational structure featured a collection of regional units with shared objectives that nonetheless operate relatively autonomously. According to internal communications, The Base organises its members into units

58 Description of tactics, techniques and procedures for chain-hopping found on a website associated with the American Futurist.
59 Ware, "Siege: The Atomwaffen Division": 10.
60 "Atomwaffen Division".
61 Alex Newhouse, "The Threat Is the Network: The Multi-Node Structure of Neo-Fascist Accelerationism," *CTC Sentinel*, Vol. 14, Issue 5, June 2021.
62 Mack Lamoureux, Ben Makuch and Zachary Kamel, "How One Man Built a Neo-Nazi Insurgency in Trump's America," *Vice News*, 7 October 2020.
63 Southern Poverty Law Center, "Louis Beam," accessed 12 June 2022, https://www.splcenter.org/fighting-hate/extremist-files/individual/louis-beam.

of three individuals to perform violent activities.[64] However, though the group was supposed to follow a cell-like structure, leader Nazzaro micromanaged the group as a whole.

According to public reporting, Nazzaro purchased secluded property in a rural portion of Washington state on behalf of The Base with the intention of using that property for paramilitary training.[65] Through a Delaware-registered company called Base Global LLC,[66] Nazzaro purchased three ten-acre parcels of undeveloped land in Ferry County for $33,000 in December 2018.[67] However, there is no publicly available information about the origins of these funds.

There is little available information about The Base's fundraising strategies. According to its defunct website, "Participation is free, but donations are welcomed to cover costs for training events and facilities."[68] However, no information was provided on how to donate. The Base allowed members to maintain affiliations with multiple groups and the focus was on training, networking and skill development. Public reporting suggests that each member was responsible for their own financing to get to training camps. There is no public information about the use of cryptocurrency by The Base.

Blood & Honour / Combat18

Since its emergence in the 1980s, Blood & Honour has used various financing methods in order to support its efforts. According to its official propaganda, the group can be found in 23 countries across Europe, North America, South America and Oceania.[69] In examining the group's digital infrastructure, one thing that is apparent is that a main propaganda vehicle for Blood & Honour is music. The Blood & Honour field manual states that "The CDs are not only a mega fundraiser for the Movement. It is also perhaps the single most important propaganda messenger",[70] which is reflective of the movement's peak in the 1990s and early 2000s. These CD propaganda vehicles acted as a source of the movement's financing. In another Blood & Honour publication, "The Way Forward", the author describes how National Socialist bands would receive royalties from Blood & Honour labels and bands received free or paid-for trips around the EU, the USA and the UK to perform their music.[71] However, after the death of the leader of Blood & Honour Ian Stuart Donaldson, there was a great deal of infighting over the royalties due to be paid out by the Blood & Honour label.

The selling of magazine subscriptions and branded merchandise also served as a source of financing.[72],[73] The Blood & Honour and Combat18 websites demonstrate a mixed bag of financing options.[74]

64 Mapping Militants team, "The Base," Stanford Center for International Security and Cooperation, February 2021, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/the-base#highlight_text_26735.
65 Nick R. Martin, "Cracking open The Base," *The Informant*, 27 January 2020. https://www.informant.news/p/cracking-open-the-base?s=r.
66 OpenCorporates, "BASE GLOBAL LLC," accessed 12 June 2022, https://opencorporates.com/companies/us_de/6867363.
67 Jason Wilson, "Revealed: the true identity of the leader of an American neo-Nazi terror group," *The Guardian*, 24 January 2020, https://www.theguardian.com/world/2020/jan/23/revealed-the-true-identity-of-the-leader-of-americas-neo-nazi-terror-group.
68 Archived version of The Base page can be found at https://web.archive.org/web/20200129035632/https://thebase765520628.wordpress.com/.
69 A list of international Blood & Honour organisations can be found at https://www.bloodandhonourworldwide.co.uk/bhww/b-h-worldwide-contacts/.
70 Max Hammer, "Blood & Honour Field Manual," *Blood & Honour Scandinavia*, 2000: 15.
71 Max Hammer, "The Way Forward," *Blood & Honour Scandinavia*, 1997: 9.
72 See https://www.bloodandhonourworldwide.co.uk/bhww/b-h-magazine/subscribe/.
73 See https://28h.hu/support/.
74 See https://www.bloodandhonourworldwide.co.uk/bhww/b-h-worldwide-contacts/.

Most chapters of Blood & Honour or Combat18 instructed members to use low-tech methods of financing, such as sending in a cheque or postal order payable to "Blood & Honour".[75] This was usually the proposed method for the purchase of magazine subscriptions. For the Blood & Honour "white cross" – the support organisation run for Blood & Honour prisoners and their families – fundraising is carried out in person by direct donations or the purchase of raffle tickets at fundraising operations held at Blood & Honour concerts and socials.[76]

There was an option to send an email for additional information for other payment options on some of the Blood & Honour / Combat18 sites, but it is unclear what those options would have been.[77] Blood & Honour and Combat18 branches that had their own music labels or were selling their music online offered a combination of online credit card payments and, in some instances, payment through PayPal. Online payments and PayPal were also the preferred methods for purchasing apparel and memorabilia. The defunct Blood & Honour France website linked to a Facebook page that acted as that branch's online shop.[78]

There does not appear to be any Blood & Honour or Combat18 manual or guide on the use of cryptocurrencies. The Blood & Honour and Combat18 manuals that are in the ICSR database do not mention any tactics, techniques or procedures regarding financing strategies. The majority of Blood & Honour branches have an email address; therefore, it is possible that an individual could send them an electronic money transfer via email or send funds peer-to-peer via a mobile payment app. The chapters that have a postal box do have instructions on how to send them a cheque or postal order. For Blood and Honour Austria, Canada and Germany, there is little available information about the groups as they are listed as terrorist entities under law. According to their official website, members from these countries are asked to contact Blood & Honour UK.

While Blood & Honour / Combat18 primarily uses more traditional methods of financing, it does incorporate newer financial technologies into its payment systems, such as PayPal and Facebook Marketplace. However, these are modest adaptations potentially made in response to user feedback rather than an effort to innovate or to obscure the source and destination of funds. The use of more traditional financing methods plausibly reflects the age of the group and its membership.

The Proud Boys

The Proud Boys is an all-male loose association of different chapters in a number of different countries that was founded in 2016 in the United States.[79] The Proud Boys regularly attend events with other groups that promote white supremacist and anti-government views, despite the fact that the Proud Boys leadership deny any affiliation with white supremacy or neo-Nazism.[80] In addition, the group is

75 See https://www.bloodandhonourworldwide.co.uk/bhww/b-h-magazine/subscribe/.
76 See https://www.bloodandhonourworldwide.co.uk/bhww/b-h-white-cross/.
77 See example from 9% production informing users that they will no longer accept payment via PayPal and all orders will be invoiced via email https://web.archive.org/web/20170420183051/http://9percentproductions.com/.
78 See https://web.archive.org/web/20130503072327/http://28hexagone.wordpress.com/hexagone-shop/.
79 Matthew Kriner and John Lewis, "Pride & Prejudice: The Violent Evolution of the Proud Boys", *CTC Sentinel* 14, no. 6, 2021.
80 Mapping Militants team, "Proud Boys," *Center for International Security and Cooperation*, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/proud-boys#text_block_32630.

semi-accelerationist in that it supports violence in preparation for civil war in the United States.[81] The majority of the group's public activities consist of protesting or attending political rallies and events, usually with the purpose of inciting violence.[82]

While it has a formal organisational structure with a national leader (chairman) and local chapter leaders, the rest of its structure is much looser. Chapters raise funds in a number of ways, such as crowdfunding (usually for specific events or issues) and through "charitable" donations (the group is not a registered charity) and membership dues.[83] The higher-level organisation raises funds from the website 1776.shop, which is owned and administered by current Proud Boys chairman Enrique Tarrio.[84] The site sells T-shirts, challenge coin and a variety of Proud Boys paraphernalia. Payment services are provided by credit card companies and CoinPayments, a cryptocurrency exchange. Tarrio also owns a T-shirt printing business that is associated with 1776.shop. He might also have made money from livestreaming on Twitch,[85] though it is unclear whether these funds were used to support Proud Boys activity or for personal profit.

There is little publicly available information on what the Proud Boys uses its money for. They plausibly spend it on travel to protests, as well as on weapons and equipment. Legal and medical fees are also popular crowdfunding causes for the group.[86] Indeed, donations have been solicited for NYC9, the group's legal defence fund.[87]

Little information exists on how the Proud Boys organisation or chapters manages and stores its funds. Group funds are likely managed by Tarrio himself, though the group potentially has little use for organisational-level funding other than to support high-level members like Tarrio or others who might have been financially deplatformed from their work, online activities and so on. The group's violence usually consists of street brawls, protests, counter-protests and murders, all of which require little in the way of funding and do not require sophisticated or innovative financing mechanisms.

The Proud Boys has demonstrated little in the way of financing innovation, although as with other REMVE and AGAAVE groups, it tends to use propaganda sales to fund some of its activities and leadership. Payment services provided to sites selling propaganda do use fintech, such as crowdfunding and cryptocurrencies, and some of the potential group funders demand some level of fintech capability, a possible driver of this adoption. In the REMVE and AGAAVE space, the Proud Boys is the most aggressive adopter of fintech; however, this is likely an opportunistic adaptation rather than a strategic one, since most of this adoption is focused on facilitating donations and selling propaganda rather than obscuring the source and destination of funds for its activities.

81 Kriner and Lewis, "Pride & Prejudice: The Violent Evolution of the Proud Boys", 2021.
82 Mapping Militants team, "Proud Boys".
83 Will Carless, "Proud Boys Got Donations from Chinese Americans on GiveSendGo," *USA Today*, 4 May 2021, https://www.usatoday.com/story/news/nation/2021/05/04/proud-boys-chinese-americans-community-support-donations/7343111002/.
84 April Glaser, "The Swag Shop of the Far Right," *Slate*, 7 February 2019, https://slate.com/technology/2019/02/proud-boys-1776-shop-paypal-square-chase-removed.html.
85 Kellen Browning, "Extremists Find a Financial Lifeline on Twitch," *The New York Times*, 27 April 2021, sec. Technology, https://www.nytimes.com/2021/04/27/technology/twitch-livestream-extremists.html.
86 Carless, "Proud Boys Got Donations".
87 Glaser, "The Swag Shop of the Far Right".

Russian Imperial Movement

The Russian Imperial Movement (RIM) is based in Saint Petersburg, Russia,[88] and operates in Russia, Ukraine, Syria and Libya.[89] RIM's founder claims that the group is funded by public donations.[90] The group has also raised funds through other means, such as music concerts.[91] It has an adversarial relationship with the Russian government,[92] but has worked alongside a Russian political party in the past.[93]

The group uses its funds to provide "clothes, shoes, special equipment – communications, body armor" for every militant it sends to Ukraine.[94] The group has also provided training to Swedish members of the Nordic Resistance Movement and also reportedly offered paramilitary training to organisers of the 2017 Unite the Right rally in Charlottesville, Virginia, and members of other US-based white nationalist groups.[95] RIM provided training to two Swedes who bombed a bookshop, a refugee shelter and an asylum-seeker campsite.[96] The training it offers is free for recruits.[97]

RIM also uses funds to purchase equipment for training recruits in bomb-making, marksmanship, combat medicine and small-group tactics, such as assaulting and clearing buildings.[98] It conducts military operations in Russia and Ukraine and is believed to have sent fighters to the Central African Republic, Syria and Libya.[99]

RIM also sponsors other terrorist and extremist groups using its funds and has donated money to foreign neo-Nazi and white supremacist groups, such as the Nordic Resistance Movement.[100] RIM regularly "posts updates talking about sending help to poor families, sending gifts to children in foster care, fundraising for people with serious diseases or for families of their 'brothers in arms' who were killed in military campaigns (for example, in Ukraine)."[101]

As RIM is not a banned Russian entity, it is possible that the group uses the Russian financial system to move funds within the country and to its operational units in other countries. The leader of the group, Stanislav Anatolyevich Vorobyev, plausibly manages the

88 Center for International Security and Cooperation, "Russian Imperial Movement," Mapping Militants (Stanford University, 2021), https://cisac.fsi.stanford.edu/mappingmilitants/profiles/russian-imperial-movement.
89 Counter Extremism Project, "Russian Imperial Movement (RIM)," 2020, https://www.counterextremism.com/threat/russian-imperial-movement-rim.
90 ibid.
91 Natalia Yudina and Vera Alperovich, "Old Problems and New Alliances: Xenophobia and Radical Nationalism in Russia, and Efforts to Counteract Them in 2016," Racism and Xenophobia (SOVA Center for Information and Analysis, 5 August 2017), http://www.sova-center.ru/en/xenophobia/reports-analyses/2017/05/d36995.
92 Daveed Gartenstein-Ross, Samuel Hodgson and Colin P. Clarke, "The Russian Imperial Movement (RIM) and Its Links to the Transnational White Supremacist Extremist Movement," *ICCT*, 24 April 2020, https://icct.nl/publication/the-russian-imperial-movement-rim-and-its-links-to-the-transnational-white-supremacist-extremist-movement/.
93 Elizabeth Grimm Arsenault and Joseph Stabile, "Confronting Russia's Role in Transnational White Supremacist Extremism," *Just Security* (blog), 6 February 2020, https://www.justsecurity.org/68420/confronting-russias-role-in-transnational-white-supremacist-extremism/.
94 Counter Extremism Project, "Russian Imperial Movement (RIM)".
95 Gartenstein-Ross et al., "The Russian Imperial Movement".
96 Public Safety Canada, "Currently Listed Entities," 3 February 2021, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx#511.
97 Stanislav Vorobyev, "Координатор тренировочной базы ополченцев: Ни один наш боец не видел ни одного представителя Интербригад," 30 January 2015, https://www.zaks.ru/new/archive/view/135459.
98 Counter Extremism Project, "Russian Imperial Movement (RIM)": 3.
99 The Soufan Center, "Inside The Russian Imperial Movement: Practical Implications of U.S. Sanctions," Special Report, 23 April 2020, https://thesoufancenter.org/research/inside-the-russian-imperial-movement-practical-implications-of-u-s-sanctions/.
100 Public Safety Canada, "Currently Listed Entities"; Ezel Sahinkaya and Danila Galperovich, "Radical Russian Imperial Movement Expanding Global Outreach," VOA (blog), 9 May 2020, https://www.voanews.com/a/extremism-watch_radical-russian-imperial-movement-expanding-global-outreach/6189020.html
101 Anna Kruglova, "'For God, for Tsar and for the Nation: Authenticity in the Russian Imperial Movement's Propaganda,'" *Studies in Conflict & Terrorism*, 19 October 2021: 1–23, https://doi.org/10.1080/1057610X.2021.1990826.

group's funds.[102] Alexander Zuchkovsky serves as the head of logistics for RIM, promoting the separatist cause in Ukraine and recruiting foreign fighters to join the conflict.[103] He potentially also plays a role in managing the group's finances. He is alleged to have organised "30 million rubles worth of shipments of weapons and military equipment to Ukrainian separatists"[104] and led an operation to send supplies, including radios, uniforms, mobile phones, drones, binoculars and even items as banal as soap, batteries and toothpaste, to support the fighters. In 2014 he told *Der Spiegel* that he had raised about $485,000 for the effort.[105]

The group does not appear to have innovated in terms of any of its financial activities; instead, it uses existing methods such as donations from identity-based support networks, propaganda and music festivals to raise funds. There are significant informational gaps in how the group moves and stores its funds, which could shed light on any potential innovation in this space. However, since the group enjoys relative impunity in Russia, it is likely able to take advantage of the financial system in Russia to finance some or most of its activities. Since cryptocurrencies and other fintech are in use in Russia, this could include some fintech adoption.

Three Percenters

The Three Percenters (also known as III%ers and Threepers) is an ideological movement and part of the broader militia movement that claims that only 3% of American colonists fought against the British during the American Revolution.[106] Members subscribe to the idea that they are part of a small number of dedicated patriots protecting Americans from government tyranny, as the 3% did before them.

The group has received support from such organisations as the American Defense Force and the American Border Foundation, which allegedly helped to sponsor rallies.[107] The American Border Foundation was a 501(c)(3) non-profit in the United States, granted tax-exempt status in 2018 and was determined to be a public charity under United States law. In 2022, the organisation's federal tax-exempt status was automatically revoked for not filing the appropriate forms. Other non-profit organisations suspected to be associated with the group were also set up to receive donations through the Amazon Smile programme.[108] This allows donations to charities as well as the donation of items needed by charities. The Three Percenters might also raise money from propaganda sales on its websites. Payments on the website can be made

102 Center for International Security and Cooperation, "Russian Imperial Movement," Mapping Militants (Stanford University, 2021), https://cisac.fsi.stanford.edu/mappingmilitants/profiles/russian-imperial-movement.
103 ibid.
104 Counter Extremism Project, "Russian Imperial Movement (RIM)": 2.
105 Robin Dixon, "Inside White-Supremacist Russian Imperial Movement, Designated Foreign Terrorist Organization by U.S. State Department," *Washington Post*, 13 April 2020, https://www.washingtonpost.com/world/europe/russia-white-supremacist-terrorism-us/2020/04/11/255a9762-7a75-11ea-a311-adb1344719a9_story.html.
106 Southern Poverty Law Center, "Three Percenters," accessed 3 June 2022, https://www.splcenter.org/fighting-hate/extremist-files/group/three-percenters.
107 Alejandro J. Beutel and Hatewatch Staff, "Antigovernment Militia Leader Organizing Nationwide Protests This Weekend," Southern Poverty Law Center (blog), 21 February 2019, https://www.splcenter.org/hatewatch/antigovernment-militia-leader-organizing-nationwide-protests-this-weekend.
108 Laura Hautala, "Militia-Related Nonprofits Listed Among Groups That Can Receive Amazon Smile Donations," *CNET*, 20 January 2021, https://www.cnet.com/tech/tech-industry/militia-related-nonprofits-listed-among-groups-that-can-receive-amazon-smile-donations/.

through credit and debit card, as well as PayPal. The group also has connections to politicians; however, it is currently unclear whether it is financially supported by political elites.[109]

The Three Percenters was founded by Mike Vanderboegh, "an Alabama-based anti-government extremist who had been involved in the militia movement for many years".[110] The movement is divided into a number of key figures and organisations, such as the III% Security Force (led by marine veteran Chris Hill), American Patriots III% (led by Scott Seddon), III% United Patriots (founded by Mitch Nerem and marine veteran Mike Morris) and III% Georgia Martyrs (led by Justin Thayer).[111] These groups are further organised into local, state and regional chapters and use a paramilitary structure to organise themselves, coordinate actions and make decisions.[112] This structure potentially also extends to financial matters and most chapters probably finance their activities themselves through donations from members. The Three Percenters has "been linked to bomb plots targeting United States federal government buildings and Muslim communities".[113] How these plots were financed is currently unknown.

The movement also uses advertisements to sell merchandise on Facebook and Google;[114] these merchandise sales potentially have the added benefit of acting as a soft recruitment tool. The group has also hosted rallies and events against lockdown measures related to the coronavirus pandemic and in support of Donald Trump.[115] Members buy weapons, bomb-making equipment, ammunition and Three Percenter merchandise.[116] Individual members purchase items such as military gear, communications equipment and weapons to intimidate others and attempt operations.[117] Individual chapters also use funds to conduct paramilitary training and vigilante border patrols along the United States–Mexico border.[118],[119]

Given its non-proscribed status in the United States, the Three Percenters potentially uses only basic tradecraft to hide the source and destination of funds, if at all. However, its use of non-profit and charitable organisations can serve to obfuscate its activities. For instance, one man associated with the group "ran a nonprofit called the American Phoenix Project, which was classified under educational services and schools, but was used to organise rallies in support of former President Donald Trump leading up to the Jan. 6 insurrection." This organisation is in the process of being dissolved. Another Three Percenter, Eric Parker, founded the

109 Katie Rogers and Dave Philipps, "A Republican Lawmaker for Whom the Spectacle Is the Point," *The New York Times*, 14 January 2021, sec. U.S., https://www.nytimes.com/2021/01/13/us/politics/lauren-boebert-republican.html.
110 ADL, "Three Percenters," Backgrounder, 13 July 2020, https://www.adl.org/resources/backgrounders/three-percenters.
111 Southern Poverty Law Center, "Three Percenters".
112 ibid; Spencer Sunshine, "Profile on the Right: Three Percenters," Political Research Associates (blog), 5 January 2016, https://politicalresearch.org/2016/01/05/profiles-on-the-right-three-percenters.
113 Southern Poverty Law Center, "Three Percenters".
114 Jeremy B. Merrill, "Tech Firms Profited from Far-Right Militia Content Despite Ban on 'Three Percenters'," *The Markup*, 21 January 2021, https://themarkup.org/news/2021/01/21/tech-firms-profited-from-far-right-militia-content-despite-ban-on-three-percenters.
115 Southern Poverty Law Center, "Three Percenters".
116 ibid.
117 Alan Feuer and Matthew Rosenberg, "6 Men Said to Be Tied to Three Percenters Movement Are Charged in Capitol Riot," *The New York Times*, 10 June 2021, sec. U.S., https://www.nytimes.com/2021/06/10/us/politics/three-percenter-capitol-riot.html.
118 Southern Poverty Law Center, "Three Percenters".
119 ADL, "Three Percenters".

Real 3% of Idaho as an unincorporated non-profit organisation.[120] The group is able to operate with impunity in the United States, meaning that it is able to make use of the formal financial system and several tools to obscure its funds.

While the Three Percenters does not display a high degree of innovation in its financing, its use of non-profit and charitable entities is significant. This type of financing activity has also been observed among other terrorists and extremists, although the extent to which the Three Percenters is able to exploit the US charitable registration system and obtain tax exempt status is unique among REMVE and AGAAVE actors and jihadists.

120 Jason Wilson, "Idaho Candidate for Governor Endorsed by Rightwing Militia Leader, Video Reveals," *The Guardian*, 9 June 2021, sec. US news, https://www.theguardian.com/us-news/2021/jun/09/janice-mcgeachin-idaho-lieutenant-governor-rightwing-militia-leader.

6. A Look at Non-proscribed Threat Actors and the Post-organisational Landscape

The use of cryptocurrencies by REMVE and AGAAVE actors is becoming more prominent among post-organisational violent extremist and terrorist (POVET) milieus.[121] POVET refers to "violent extremism or terrorism where the influence or direction of activity is ambiguous or loose".[122] The concept is designed to be group-agnostic and is instead shaped around analysing content and actors who are influential to violent extremism and terrorism beyond those who have been proscribed by governments.[123] This is reflective of the shift in the REMVE and AGAAVE space away from groups and more towards a leaderless resistance model. Actors in the POVET space are opportunists, seeking to leverage extremists of all stripes (for example, neo-Nazis, neo-fascists, fundamentalist Christians, anarchists, Black liberationists, anti-government extremists, ethno-nationalists, eco-radicals, jihadists and even conspiracy theorists). Such a wide-reaching and inclusive framework of recruitment and engagement creates a fertile ground for innovation due to the intersection of various milieus that creates ever-changing and evolving feedback loops of varied world-views that are seemingly at odds with one another. Cynthia Miller-Idriss and Brian Hughes have called this "blurry ideologies", which highlights how diverse and even conflicting ideologies are providing a communal mechanism by which support and goals are advanced around a set of abstract virtues or beliefs that cut across traditional ideological boundaries.

Neo-Fascist Accelerationism

Examples of neo-fascist accelerationist networks include the United Acceleration Front and the National Socialist Coalition, which rapidly formed and collapsed just as quickly.

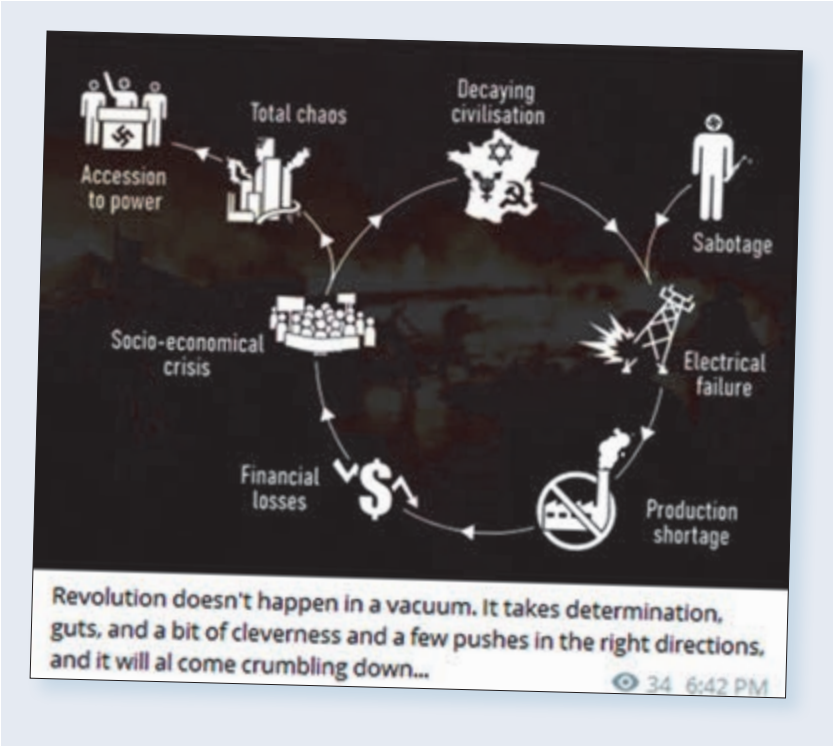
Part of why neo-fascist accelerationists are interested in fintech is tactical, based on the pseudo-anonymity afforded by the use of, for instance, cryptocurrencies. Most of these channels have Monero wallets to which users can donate and have shared the guide from the American Futurist on how to use Monero. However, the use of cryptocurrency is also ideological in neo-fascist accelerationist

121 Jacob Davey, Milo Comerford, Jakob Guhl, Will Baldet and Chloe Colliver, "A Taxonomy for the Classification of Post-Organisational Violent Extremist & Terrorist Content," *ISD*, 9 December 2021, https://www.isdglobal.org/wp-content/uploads/2022/01/A-taxonomy-for-the-classification-of-post-organisational-terrorist-content.pdf.
122 ibid.
123 ibid.

circles.[124] Neo-fascist accelerationists focus on accelerating the inevitable fall of liberal democracy: "Militant accelerationism is a set of tactics and strategies designed to put pressure on and exacerbate latent social divisions, often through violence, thus hastening societal collapse."[125] Accelerationists seek to restore society to a framework based on tradition and hierarchy; neo-fascist accelerationists advocate random acts of terrorism in an effort to ignite a chain reaction of social unrest and bloodshed. Part of the lure for REMVE and AGAAVE actors in these milieus is that they believe by not participating in the fiat system and by promoting cryptocurrencies they will be able to ultimately deal a blow to the "Jewish" banks and therefore crash the financial system.

124 H. E. Upchurch, "The Iron March Forum and the Evolution of the 'Skull Mask' Neo-Fascist Network," *CTC Sentinel* 14, no. 10; Alex Newhouse, "The Threat Is the Network: The Multi-Node Structure of Neo-Fascist Accelerationism," *CTC Sentinel* 14, no. 5.

125 Matthew Kriner on behalf of the ARC Steering Committee, "An Introduction to Militant Accelerationism," Acceleration Research Consortium, accessed 12 June 2022, https://www.accresearch.org/shortanalysis/an-introduction-to-militant-accelerationism.



Nordic Resistance Movement

The Nordic Resistance Movement (NRM) has published a cryptocurrency action plan "to prepare ourselves for an economic crisis".[126] This plan is rooted in three things. First, it draws influence from the conspiracy theories of the Great Reset and the New World Order, and that the "fake pandemic" is the first step in the coming economic crisis.[127] Second, adherents of the group also believe that, by using cryptocurrencies, for the "first time in history we have the chance to deny Jews money and use our own".[128] Third, the NRM has had, according to the action plan, "bad experiences" with bank accounts.[129] Thus the group's logic is that if there is an economic collapse, the NRM network will have access to funds that it can use to purchase necessities.[130] Similar to neo-fascist accelerationists, the group also perceives cryptocurrencies as a way of attacking the system: "Have you been fucked by the system? Fuck the system and use Monero!"[131]

The action plan also provides basic instructions and advice on how to mine cryptocurrency. It suggests the currency group members should use is Monero, as this will provide a mechanism to hide "their wealth" and is a privacy-focused coin. The plan also promotes Monero as it was not ASIC-resistant at the time,[132] thus making it easier to mine.[133]

126 Nordic Resistance Movement, "Cryptocurrency Action Plan," Telegram, 16 December 2020.
127 ibid.
128 ibid.
129 ibid.
130 The group does not take into account the challenges of cashing out Monero during an economic crisis.
131 Nordic Resistance Movement, "Cryptocurrency Action Plan".
132 An ASIC-resistant cryptocurrency has its protocol and mining algorithm configured in such a way that using ASIC machines to mine the coin is either impossible or brings no significant benefit when compared to traditional GPU mining. In some cases, using ASICs on ASIC-resistant cryptocurrencies may be even worse than using more conventional hardware. For more information, see https://academy.binance.com/en/glossary/asic-resistant.
133 As of December 2019, Monero has upgraded to RandomX, a mining algorithm that aims to be ASIC-resistant.

It explains how to create a mining pool to mine for Monero and suggests that leaders of cells and groups should implement a mining pool to generate an influx of Monero for the movement. The plan also recommends the use of Ragerx.lol as the easiest way to implement a mining pool on a member's computer.[134]

From NRM's perspective, cryptocurrencies are a technology that the group can use to fight the system but one that members need to educate themselves about prior to actually implementing. Based on an analysis of this action plan, it appears that this is more of a warning sign of adaptation yet to come than an example of current use.

134 RagerX is a miner, an operating system and a pool that boots off a thumbdrive. See: https://ragerx.lol/.

7. Cryptocurrency and Funding Terrorism and Extremism

Despite the general fear that cryptocurrencies would become a central source of terrorist financing and contribute to the funding of actual terrorist attacks, there is scarce evidence that this is the case. In the aftermath of Islamic State's November 2015 Paris attacks, there were reports that the attack had been funded partly through bitcoin, but these reports have never been confirmed. Similar reports circulated following the terrorist attacks in Sri Lanka in Easter 2019, although these reports were determined to be unfounded.[135] One of the only known cases of cryptocurrency being used to finance an attack is the July 2016 attack against the Solo Police Headquarters in Indonesia. According to reports, the mastermind behind the attack, a deceased Syrian-based militant named Bahrun Naim, used PayPal and bitcoin to transfer funds for the attack. Although the total amount sent by Naim to fund the attack was relatively small – less than $1,000 – it represents an innovation in jihadist operational financing.[136] In other recent attacks from the REMVE and AGAAVE space, attackers have eschewed the use of cryptocurrencies but have still made use of other fintech, such as PayPal, to finance their attacks. For instance, the Buffalo shooter used money he had in his bank account and his PayPal account to fund some of his weapons and equipment purchases. However, he also sold some of his personal belongings at flea markets to raise money to make further purchases and specifically avoided using cryptocurrency for any financing of his attack.[137]

There are a number of reasons why cryptocurrency and, to a lesser extent, other financial technologies have not been used to finance jihadist attacks. These reasons extend across the political and ideological spectrum to all types of groups. First, there remain some technological barriers to using cryptocurrency. While cryptocurrency has been in existence for over a decade, obtaining cryptocurrency in some jurisdictions remains challenging. Many banks prohibit the sending of funds to exchanges and some countries have started to ban cryptocurrency ATMs.[138] As the glossary at the beginning of this handbook illustrates, there is technical language that needs to be understood to acquire cryptocurrency and even greater barriers to truly anonymous use. Second, cryptocurrency transactions can be slow and costly, making the transfer of relatively small sums of money prohibitively expensive and time-consuming, particularly in the presence of other, more reliable methods, such as the formal financial system, money-service businesses, *hawalas* and cash couriers. Thirdly, cashing out cryptocurrency into state-backed currency or using it to purchase weapons or device components for attacks can

135 Jessica Davis, "A Canadian Cryptocurrency Caper in the Sri Lanka Attack? Unlikely," INTREPID (blog), 6 May 2019, https://www.intrepidpodcast.com/blog/2019/5/6/a-canadian-cryptocurrency-caper-in-the-sri-lanka-attack-unlikely.
136 V. Arianti and Kenneth Yeo Yaoren, "How Terrorists Use Cryptocurrency in Southeast Asia," *The Diplomat*, 30 June 2020.
137 Jessica Davis, "Buffalo Shooting: Financing Terrorism," Substack newsletter, Insight Intelligence (blog), 17 May 2022, https://insightintel.substack.com/p/buffalo-shooting-financing-terrorism.
138 See: https://www.bbc.com/news/technology-60709209.

be technologically challenging and time-consuming, and can open a user up to potential theft. While "informal" exchanges are starting to expand into cryptocurrencies in places like Syria and Afghanistan, this is still limited. Finally, many cryptocurrencies are extremely volatile, making them impractical as a transfer mechanism for funds.

Over the next few years, the use of cryptocurrencies by jihadists and REMVE and AGAAVE actors to fund attacks is likely to remain limited and largely within the purview of more technologically sophisticated plotters. Some extremists might seek to purchase cryptocurrencies as a form of investment, the proceeds of which could be used to fund attacks or a terrorist organisation. However, given the current volatility and low price of many of these speculative assets, this is unlikely to materialise in the near term and would likely be a longer-term financing strategy. Despite these limitations, counterterrorism professionals will need to maintain situational awareness of cryptocurrencies and fintech, as their adoption is likely to grow over time in line with increased societal adoption.

8. Countering the Financing of Terrorism and Extremism Using New Financial Technologies

Countering extremist and terrorist financing using cryptocurrency and other financial technologies has unique challenges. In some cases, fintech like PayPal are considered to be payment processors rather than money-service businesses, which means that they fall outside anti-money-laundering and counterterrorist financing regulatory processes in some jurisdictions. Some of these technologies, including cryptocurrency exchanges, have been reluctant to implement know-your-customer or know-your-client regulations, meaning that even when regulation is in place, it is enforced unevenly. Furthermore, jurisdictions have different regulations around cryptocurrency and fintech, meaning that terrorists and extremists can engage in geo-financial arbitrage, essentially choosing to focus their financing activities (such as the storage and movement of funds) in or through jurisdictions with lax regulations (this is true in other contexts outside the use of fintech as well, as the popularity of such financial centres as Dubai illustrate).[139]

In some cases, the use of cryptocurrencies can make transactions easier to follow and might not require the level of authorisation usually associated with tracking financial transactions, such as judicial warrants. Blockchain-analytics companies are increasingly able to exploit the blockchain using techniques such as clustering to identify, de-anonymise and attribute wallets and transactions to particular individuals or entities. At the same time, illicit actors are developing obfuscation techniques, such as mixers or tumblers, chain-hopping and privacy coins, in a cycle of adaptation and counter-adaptation. Both of these processes are facilitated by the open and public nature of the blockchain, which in turn accelerates these innovations and adaptations (in traditional terrorist and extremist financing, innovation and adaptation has generally followed only after successful court proceedings or disruptions that have revealed the counter-financing methods employed). While blockchain-analytics companies can be force multipliers for counterterrorism and counter-extremism finance practitioners, illicit actors also potentially make use of the same tools and techniques in an effort to enhance their anonymity and obfuscate the source and destination of their funds, particularly those that have invested in cryptocurrency capabilities.

139 Matthew T. Page and Jodi Vittori, "Dubai's Role in Facilitating Corruption and Global Illicit Financial Flows" (Carnegie Endowment for International Peace, 2020).

9. Understanding and Anticipating Terrorist and Extremist Financing Adaptation and Innovation

The majority of terrorist groups, cells and individuals adopt new technologies, tactics, techniques and procedures gradually. Few groups or entities truly innovate in the finance space, as finance is more constrained by external factors (like existing banking systems) than other areas of potential innovation and adaptation (such as attack tactics, for example). Terrorist financing is resistant to high levels of innovation because most terrorist actors are constrained by the financial and economic systems in which they operate. They are at the mercy of existing structures. As such, shifts in terrorist financing trends and methods are best seen as adaptation rather than innovation and as a learning process. This process is also largely accompanied by changes in global or local financial and economic systems.

Despite the slow march of financial adaptation by terrorists, it is important to think about innovation and adaptation in terrorist organisations and entities in terms of non-violent activity (like financing) in order to anticipate changes in methods and mechanisms.[140] For most terrorists, adaptation of new financing techniques emerges when changes to economic and financial systems occur. For instance, terrorists exploit fintech and cryptocurrencies when it becomes expedient for them to do so and when such technologies become widely accepted and used. Until then, innovation can occur among motivated individuals or cells, but new financing methods are rarely pursued by groups or more established cells or organisations.

While other forms of terrorist innovation are often linked to problem-solving and efforts to circumvent countermeasures,[141] terrorist financing innovation is relatively immune to these pressures. For instance, even twenty years after the global community implemented counterterrorist financing policies and practices on a macro-scale,[142] terrorist actors continue to use banks, cash couriers, trade-based mechanisms and money service businesses to move funds.[143] There has been little change in the primary methods used by terrorists to move funds.

Unlike other aspects of innovation, terrorist financial innovation and adaptation does potentially allow for the development of some predictive indicators.[144] These indicators will all be jurisdictionally and geographically specific, depending on the financial and economic

140 Rashmi Singh, "A Preliminary Typology Mapping Pathways of Learning and Innovation by Modern Jihadist Groups," *Studies in Conflict & Terrorism* 40, no. 7 (3 July 2017): 624–44, https://doi.org/10.1080/1057610X.2016.1237228.
141 Lubrano, "Navigating Terrorist Innovation".
142 Jessica Davis, "Understanding the Effects and Impacts of Counter-Terrorist Financing Policy and Practice," *Terrorism and Political Violence* 0, no. 0 (9 June 2022): 1–17, https://doi.org/10.1080/09546553.2022.2083507.
143 Jessica Davis, *Illicit Money*: 221.
144 Lubrano, "Navigating Terrorist Innovation".

terrain where a terrorist entity or organisation operates or seeks to operate.[145] Terrorists will prioritise adoption of new technologies where there is an operational security advantage to doing so (as a means to obscure the source, destination or use of funds). They will also adopt new technologies when there is sufficient market saturation to allow them to use the technology easily and sufficient users among which they can hide. Terrorists will prioritise new technologies that allow them to quickly, easily and cheaply move money, both domestically and internationally, or that allow them to buy the goods and services they require.

The information in this workbook is intended to familiarise researchers, analysts and practitioners with how different types of terrorist actors use fintech and cryptocurrencies to facilitate their financial activities. The process of terrorist adoption of fintech is laid out for various groups and can serve as a framework to help analysts to predict if or when a particular group or terrorist actor might adopt particular fintech or cryptocurrencies. This analysis should keep in mind the broader economic and financial context where terrorist actors are operating and whether fintech and cryptocurrencies are viable options for facilitating financial transactions. Beyond this, the workbook contains information (such as keywords) that can be used to search through information holdings for any indication of cryptocurrency or financial technology adoption by terrorists, thus providing early warning of terrorist adaptation.

145 Davis, *Illicit Money*.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. +44 20 7848 2098
E. mail@icsr.info

Twitter: @icsr_centre

Like all other ICSR publications, this report can be downloaded free of charge from the ICSR website at **www.icsr.info**.