Centar za sigurnosne studije - BIH

Centre for Security Studies - BH

Raising awareness about the increased threat of the criminal and terrorist use of cryptocurrencies

2022

Centar za sigurnosne studije - BIH

Centre for Security Studies - BH

Raising awareness about the increased threat of the criminal and terrorist use of cryptocurrencies

Author: Nicolò Miotto

Nicolò Miotto is currently pursuing the International Master in Security, Intelligence & Strategic Studies (IMSISS) awarded by a consortium of European universities – University of Glasgow (UK); Dublin City University (Ireland); Charles University in Prague (Czech Republic). He is Adjunct Professor at Università degli Studi Niccolò Cusano (Rome) where he teaches courses on war crimes, crimes against humanity and genocide. His research interests include terrorism and violent extremism, emerging technologies, international law and geopolitics.

April, 2022

Table of contents

List of abbreviations

AML – anti-money-laundering

BT – blockchain technology

CSAM – child sexual abuse material

CTF – counter terrorism financing

EUROPOL – European Union Agency for Law Enforcement Cooperation

FATF – Financial Action Task Force

ID – identity document

ICT – International Institute for Counter-Terrorism

IP – Internet Protocol

TOR – The Onion Router

Executive summary

- *Criminal and terrorist organisations are increasingly using cryptocurrencies*, thus leading to emerging threats in the cyberspace.
- *Money-laundering, tax evasion, ransomware extortion, trading in illicit goods and services, purchasing of child sexual abuse material and terrorist financing* are concerning criminal and terrorist activities involving the use of cryptocurrencies.
- *Bitcoin and Monero are the most used cryptocurrencies* among both criminals and terrorists, however *other cryptocurrencies such as Litecoin, Dash and Ethereum are being growingly used* in criminal and terrorist financial activities.
- *The anonymity/pseudo-anonymity and security characterising cryptocurrencies can challenge law enforcement investigative efforts* aimed at countering criminal and terrorist activities.
- *There has not been a widespread adoption of cryptocurrencies by terrorist and criminals yet*, however this is likely to change in the next future.

Introduction

Money and financial resources are fundamental factors shaping and supporting the activities of both criminal and terrorist organisations. Among diverse mechanisms and means of criminal and terrorist financing, cryptocurrencies are becoming assets of increased importance. From the Latina American crime and drug cartels to the Italian mafia (e.g., *Camorra*, and *'ndrangheta*), these cutting-edge technologies are growingly being used by criminals and terrorists,[1] thus constituting a threat to national security and public safety.

These technologies are attracting the interests of malevolent actors due to their advantageous characteristics including anonymity and security, global reach, high speed of transfers, non-repudiation and low-cost of transactions, and user-friendly nature.[2] In the last decade, the threats deriving from the criminal and terrorist use of cryptocurrencies have been growing.[3] Particularly, cryptocurrencies are facilitating criminal and terrorist money-laundering processes, the finance of illegal activities, and the purchase of illicit goods and services.[4] Cryptocurrencies pose then an increased terrorist risk due to the interlinks between criminal and terrorist use of these technologies.[5]

Counter terrorism financing (CTF) has been mainly concerned with tracking money flows through bank accounts and preventing financial transactions aimed at supporting terrorist activities. Since 9/11, law enforcement and intelligence agencies have significantly implemented CTF measures, disrupting fundraising networks and severely affecting the financial activities of terrorist organisations.[6] However, since the 2010s, terrorist groups like Al-Qaeda and Hamas have been developing alternative means to finance their activities, using, for example, electronic payments.[7]

---

[1] Peter Seele, "Let Us Not Forget: Crypto Means Secret. Cryptocurrencies as Enabler of Unethical and Illegal Business and the Question of Regulation," *Humanistic Management Journal* 3, no. 1 (May 30, 2018): 133–39, https://doi.org/10.1007/s41463-018-0038-x; Diego Oré, "Latin American Crime Cartels Turn to Cryptocurrencies for Money Laundering," *Reuters*, December 8, 2020, https://www.reuters.com/article/mexico-bitcoin-insight-idUSKBN28I1KD.

[2] Alan Brill and Lonnie Keene, "Cryptocurrencies: The next Generation of Terrorist Financing?," *Defence against Terrorism Review* 6, no. 1 (January 15, 2014): 7–30, https://ssrn.com/abstract=2814914.

[3] Steven David Brown, "Cryptocurrency and Criminality," *The Police Journal: Theory, Practice and Principles* 89, no. 4 (August 3, 2016): 327–39, https://doi.org/10.1177/0032258x16658927.

[4] Chad Albrecht et al., "The Use of Cryptocurrencies in the Money Laundering Process," *Journal of Money Laundering Control* 22, no. 2 (May 7, 2019): 210–16, https://doi.org/10.1108/jmlc-12-2017-0074; Kayla Izenman and Rick McDonell, "RUSI-ACAMS Cryptocurrency Risk & Compliance Survey" (Royal United Services Institute (RUSI); Association of Certified Anti-Money Laundering Specialists (ACAMS), 2020), https://www.acams.org/en/ACAMS-RUSI-Crypto-Survey-Report.

[5] Hannarae Lee and Kyung-Shick Choi, "Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework," *Victims & Offenders* 16, no. 3 (February 16, 2021): 363–84, https://doi.org/10.1080/15564886.2020.1835764.

[6] Cynthia Dion-Schwarz, David Manheim, and Patrick B. Johnston, "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats" (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR3026.html.

[7] John Hunt, "The New Frontier of Money Laundering: How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and How Governments Are Trying to Stop Them," *Information & Communications Technology Law* 20, no. 2 (June 2011): 133–52, https://doi.org/10.1080/13600834.2011.578933.

Cryptocurrencies represent one of these alternative means. Since 2017, when an Islamic State-related case of terrorist financing through cryptocurrencies was reported in Indonesia, these technologies are being monitored by law enforcement and intelligence agencies.[8] Although cryptocurrencies still constitute a small part of terrorist activities and not existing cryptocurrency can comprehensively meet terrorist organisations' financial needs,[9] this might change in the next future as a more widespread adoption of cryptocurrencies by terrorist organisations is likely.

[8] David Carlisle, "Cryptocurrencies and Terrorist Financing: A Risk, but Hold the Panic," *Rusi.org* (blog), 2017, https://rusi.org/explore-our-research/publications/commentary/cryptocurrencies-and-terrorist-financing-risk-hold-panic.
[9] Joshua Baron et al., *National Security Implications of Virtual Currency : Examining the Potential for Non-State Actor Deployment* (Santa Monica, Calif.: Rand National Defense Research Institute, 2015), https://www.rand.org/pubs/research_reports/RR1231.html; Cynthia Dion-Schwarz, David Manheim, and Patrick B. Johnston, "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats" (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR3026.html.

Brief overview on cryptocurrency and blockchain technology

The Financial Action Task Force (FATF) defines a virtual currency as

> *a **digital representation of value** that can be digitally traded and functions as (1) a **medium of exchange**; and/or (2) a **unit of account**; and/or (3) a **store of value**, but **does not have legal tender status** in any jurisdiction.*[10]

It is fundamental to distinguish virtual currency from e-money, '*which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency.*'[11]

Cryptocurrencies, a type of virtual currency, can be divided in two sub-categories: **convertible** and **non-convertible** virtual currencies.[12] The first sub-group can be exchanged for fiat currency, while the second one cannot. **Cryptocurrency exchanges** such as *Bitfinex* and *Coinbase* allow users to buy and sell virtual currencies that can be converted into fiat currency against the payment of a commission.[13] Currently, more than 2,000 cryptocurrencies exist, but the most used are the following:[14] bitcoin (BTC), ethereum (ETH), ripple (XRP), bitcoin cash (BCH), litecoin (LTC), stellar (XLM), cardano (ADA), IOTA (MIOTA), NEO (NEO), monero (XMR), and dash (DASH). Trends in prices of the mentioned cryptocurrencies can be viewed on websites such as *CoinMarketCap* and *Trading View*.[15]

Cryptocurrencies present numerous characteristics but **anonymity and privacy** are the most important. The degree of anonymity and privacy provided depends on the cryptocurrency adopted. While BTC can offer pseudo-anonymity since its users are identified by public keys and transactions can be linked to real world identities, other cryptocurrencies such as DASH and especially XMR offer higher levels of privacy and anonymity.[16]

---

[10] Financial Action Task Force (FATF), "Virtual Currencies - Key Definitions and Potential AML/CFT Risks" (Financial Action Task Force (FATF), 2014), https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 4.

[11] Financial Action Task Force (FATF), "Virtual Currencies - Key Definitions and Potential AML/CFT Risks" (Financial Action Task Force (FATF), 2014), https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 4.

[12] Financial Action Task Force (FATF), "Virtual Currencies - Key Definitions and Potential AML/CFT Risks" (Financial Action Task Force (FATF), 2014), https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 4.

[13] Robby Houben and Alexander Snyers, "Cryptocurrencies and Blockchain" (Policy Department for Economic, Scientific and Quality of Life Policies, 2018), https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf, 26.

[14] Robby Houben and Alexander Snyers, "Cryptocurrencies and Blockchain" (Policy Department for Economic, Scientific and Quality of Life Policies, 2018), https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf, 30.

[15] The websites are available at the following links: Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap; Cryptocurrency Market — TradingView.

[16] Niluka Amarasinghe, Xavier Boyen, and Matthew McKague, "A Survey of Anonymity of Cryptocurrencies," in *Proceedings of the Australasian Computer Science Week Multiconference* (Association for Computing Machinery, 2019), https://doi.org/10.1145/3290688.3290693.

Cryptocurrencies run on **blockchain**.[17] Blockchain technology (BT) is a peculiar type of **distributed ledger technology**, an instrument used to record and share data across multiple data stores.[18] BT offers core advantages to users as it provides highly accurate, fast and immutable transactions, does not need intermediaries or third parties for data transfers, and relies upon complex algorithmic verification methods that increase its security.[19] Moreover, the decentralized and cryptography nature of BT allows for a higher degree of anonymity compared to traditional systems.[20]

Trends in the criminal use of cryptocurrencies

In the last decade both scholars and policymakers have emphasised that the criminal use of cryptocurrencies has been a small but prominent facet of cybercrime.[21] Although fiat currencies and cash have remained the main means of criminal financing, there have been cases of cryptocurrencies-related illegal activities such as the darknet markets *Silk Road*, *AlphaBay* and *Hansa*, the trade of illicit goods and services and cryptocurrencies ransomware and scams.[22]

Illicit darknet markets are prominent examples of cryptocurrencies-related cybercriminal activities. *Silk Road* and *AlphaBay* are infamous cases of such activities. The first had around 14,000 listings for illicit goods and services,[23] while the second had over 200,000 buyers and 40,000 sellers, featuring more than 250,000 listings for illegal drugs and chemicals.[24] *Silk Road*, together with other minor unlawful Darknet market places such as *Cloud 9* and *Hydra*, was taken down during the 2014-2015 joint law enforcement *Operation Onymous*.[25]

---

[17] Robby Houben and Alexander Snyers, "Cryptocurrencies and Blockchain" (Policy Department for Economic, Scientific and Quality of Life Policies, 2018), https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.

[18] Ibid.

[19] David Rodeck and John Schmidt, "What Is Blockchain?," *Forbes Advisor*, June 9, 2021, https://www.forbes.com/advisor/investing/what-is-blockchain/.

[20] Ibid.

[21] Tom Keatinge, David Carlisle, and Florence Keen, "Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses" (Policy Department for Citizens' Rights and Constitutional Affairs, 2018), https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf; Simon Butler, "Criminal Use of Cryptocurrencies: A Great New Threat or Is Cash Still King?," *Journal of Cyber Policy* 4, no. 3 (September 2, 2019): 326–45, https://doi.org/10.1080/23738871.2019.1680720.

[22] Steven David Brown, "Cryptocurrency and Criminality," *The Police Journal: Theory, Practice and Principles* 89, no. 4 (August 3, 2016): 327–39, https://doi.org/10.1177/0032258x16658927; Department of Justice, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," *Www.justice.gov*, July 20, 2017, https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down; Emily Fletcher, Charles Larkin, and Shaen Corbet, "Countering Money Laundering and Terrorist Financing: A Case for Bitcoin Regulation," *Research in International Business and Finance* 56 (January 2021): 1–16, https://doi.org/10.1016/j.ribaf.2021.101387.

[23] Ibid.

[24] United Nations Office on Drugs and Crime (UNODC), *World Drug Report 2018* (United Nations Office on Drugs and Crime (UNODC), 2018).

[25] European Union Agency for Law Enforcement Cooperation (EUROPOL), *Internet Organised Crime Threat Assessment (IOCTA) : 2015* (The Hague: European Union Agency for Law Enforcement Cooperation (EUROPOL), 2015), https://www.europol.europa.eu/cms/sites/default/files/documents/europol_iocta_web_2015.pdf.

However, the shutdown of these activities generated a migration of vendors and buyers to other online illicit markets such as *Agora* and *Evolution*,[26] that were eventually shut down by their administrators in 2015.[27]

Moreover, criminals, including white-collar criminals, are exploiting cryptocurrencies to launder money, evade taxes, develop fraud schemes, purchase illegal commodities such as illegal arms and drugs, and buy fake identification documents (IDs) and passport.[28] In addition, criminals are trading in child sexual abuse material (CSAM) and buying cyberattack products (e.g., phishing tools, and denial of service) that are being commercialised on marketplaces on the Dark Web.[29] According to recent reports developed by *Chainalysis*, a blockchain analysis firm, in 2021 illicit addresses received a total of $14 billion in cryptocurrencies, up 79% from $7.8 billion in 2020, and there has been a 30% increase in crypto-laundering in 2021 compared to the previous year.[30]

Finally, criminals are targeting Internet users through ransomware and scamming, requesting payments in cryptocurrencies.[31] Already in 2014, the European Union Agency for Law Enforcement Cooperation (EUROPOL) was warning against the emerging trend of ransomware extorting payments in Bitcoins from individuals.[32] In the US, the Federal Trade Commission has revealed a dramatic increase in cryptocurrencies investment scams in 2020-2021.[33]

---

[26] Ibid.

[27] Nicky Woolf, "Bitcoin 'Exit Scam': Deep-Web Market Operators Disappear with $12m," *The Guardian*, March 18, 2015, https://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars; Andy Greenberg, "Agora, the Dark Web's Biggest Drug Market, Is Going Offline," *Wired*, 2015, https://www.wired.com/2015/08/agora-dark-webs-biggest-drug-market-going-offline/.

[28] Lawrence J. Trautman, "Virtual Currencies: Bitcoin & What Now after Liberty Reserve and Silk Road?," *Richmond Journal of Law & Technology* XX, no. 4 (2014), https://doi.org/10.2139/ssrn.2393537; Jason Bloomberg, "Using Bitcoin or Other Cryptocurrency to Commit Crimes? Law Enforcement Is onto You," *Forbes*, 2017, https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/?sh=7cf28343bdc4; Sesha Kethineni and Ying Cao, "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity," *International Criminal Justice Review* 30, no. 3 (February 6, 2019): 325–44, https://doi.org/10.1177/1057567719827051;

[29] Erik Silfversten et al., "Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes" (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR4418.html; Hannarae Lee and Kyung-Shick Choi, "Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework," *Victims & Offenders* 16, no. 3 (February 16, 2021): 363–84, https://doi.org/10.1080/15564886.2020.1835764; European Union Agency for Law Enforcement Cooperation (EUROPOL), "Cryptocurrencies - Tracing the Evolution of Criminal Finances" (Luxembourg: Publications Office of the European Union, 2021), https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf.

[30] Gertrude Chavez-dreyfuss, "Cryptocurrency Crime in 2021 Hits All-Time High in Value -Chainalysis," *Reuters*, January 6, 2022, sec. U.S. Markets, https://www.reuters.com/markets/us/cryptocurrency-crime-2021-hits-all-time-high-value-chainalysis-2022-01-06/; BBC News, "Crypto Money Laundering Rises 30%, Report Finds," *BBC News*, January 26, 2022, sec. Technology, https://www.bbc.com/news/technology-60072195.

[31] Nir Kshetri and Jeffrey Voas, "Do Crypto-Currencies Fuel Ransomware?," *IT Professional* 19, no. 5 (2017): 11–15, https://doi.org/10.1109/mitp.2017.3680961.

[32] European Cybercrime Center (EC3), "Police Ransomware Threat Assessment," 2014, https://www.europol.europa.eu/cms/sites/default/files/documents/policeransomware-threatassessment.pdf.

[33] Emma Fletcher, "Cryptocurrency Buzz Drives Record Investment Scam Losses," *Federal Trade Commission (FTC)* (blog), May 17, 2021, https://www.ftc.gov/news-events/blogs/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses.

A recent example of these criminal activities is the Squid Game (SQUID) cryptocurrency – whose creation was inspired by the popular South Korean Netflix series – that resulted in a major scam.[34]

However, Internet users are not the sole targets of cybercriminals. Public institutions are becoming primary targets of criminals operating in the cyberspace. For instance, in 2021 cybercriminals attacked both the Irish and the Italian healthcare system, demanding ransoms in Bitcoins.[35]

Trends in the terrorist use of cryptocurrencies

Although the terrorist use of cryptocurrencies has been claimed to be episodic,[36] there have been prominent cases of terrorist use of these technologies. Since 2014, numerous websites and Internet users connected to Jihadi organisations and supporters have been sponsoring pages and providing instructions for cryptocurrency fundraising.[37] In the 2010s in the United States, there have been arrests and legal cases concerning individuals who have attempted to financially support terrorist groups through cryptocurrencies.[38] In 2020 the US Department of Justice announced the largest seizure to date of cryptocurrencies associated with terrorist groups.[39]

Multiple organisations like Al-Qaeda, the Islamic State and Hamas have been publicising advertisement campaigns on social media and other online channels providing Bitcoin and other cryptocurrencies wallet addresses calling for donations.[40] The International Institute for Counter-Terrorism (ICT) at Herzliya, Israel, has been monitoring the cryptocurrency terrorist financing activities of groups and individuals connected to Palestinian terrorist organisations such as Hamas and the Popular Resistance Committees.[41]

---

[34] BBC News, "Squid Game Crypto Token Collapses in Apparent Scam," *BBC News*, November 2, 2021, sec. Business, https://www.bbc.com/news/business-59129466.

[35] Laura Noonan, "Ireland Defies Hackers' Bitcoin Demand over Health System," *Financial Times*, May 14, 2021, https://www.ft.com/content/ed8d3643-1966-45b5-a31c-28dcaf93a65a; Arianna Di Cori, "Gli Hacker Bloccano I Vaccini in Tilt Il Portale Del Lazio: 'Pagate Il Riscatto in Bitcoin,'" *La Repubblica*, August 2, 2021, https://www.repubblica.it/cronaca/2021/08/02/news/gli_hacker_bloccano_i_vaccini_in_tilt_il_portale_del_lazio_pagate_il_riscatto_in_bitcoin_-312647208/.

[36] Erik Silfversten et al., "Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes" (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR4418.html.

[37] Christopher Whyte, "Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise," *Studies in Conflict & Terrorism*, January 2, 2019, 1–24, https://doi.org/10.1080/1057610x.2018.1531565.

[38] David Carlisle, "Virtual Currencies and Financial Crime: Challenges and Opportunities" (Royal United Services Institute (RUSI), 2017), https://rusi.org/explore-our-research/publications/occasional-papers/virtual-currencies-and-financial-crime-challenges-and-opportunities; Lorenzo Vidino, Jon Lewis, and Andrew Mines, "Dollars for Daesh: The Small Financial Footprint of the Islamic State's American Supporters – Combating Terrorism Center at West Point," *CTC Sentinel* 13, no. 3 (March 24, 2020): 24–29, https://ctc.westpoint.edu/dollars-daesh-small-financial-footprint-islamic-states-american-supporters/.

[39] The Soufan Center, "IntelBrief: Terrorists' Use of Cryptocurrency," The Soufan Center, December 10, 2020, https://thesoufancenter.org/intelbrief-2020-december-10/.

[40] Nadine Liv, "Jihadists Use of Virtual Currency 2," *Www.ict.org.il* (International Institute for Counter-Terrorism (ICT), 2019), https://www.ict.org.il/Article/2413/Jihadists_Use_of_Virtual_Currency_2#gsc.tab=0; Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," *Www.justice.gov*, August 12, 2020, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

[41] Eitan Azani et al., "Identifying Money Transfers and Terror Finance Infrastructure," *Www.ict.org.il* (International Institute for Counter-Terrorism (ICT), 2020), https://www.ict.org.il/Article/2488/Identifying_Money_Transfers_and_Terror_Finance_Infrastructure#gsc.tab=0.

Especially, the *Izz-ad-Din al-Qassam Brigades*, the military wing of Hamas, is argued to have launched the most extensive cryptocurrency campaign organised by a terrorist group.[42] However, also other minor Jihadi groups and organisations are adopting cryptocurrencies as means of terrorist financing. For example, ICT has investigated the cryptocurrency advertisements campaigns of the Bitcoin and Cryptocurrencies Exchange Offices in the province of Idlib, Northern Syria, which are argued to be used by the jihadi organisation *Hay'at Tahrir al-Sham*.[43]

Nonetheless, Islamist groups are not the sole terrorist actors using cryptocurrencies. Far-right individuals and groups are exploiting cryptocurrencies as companies operating online payment systems (e.g., PayPal, Apple Pay, and Google Wallet) have been removing their accounts after violent actions and protests.[44] As of this, the US Southern Poverty Law Center has revealed numerous cryptocurrencies wallet addresses related to far-right individuals and organisations.[45]

Factors behind the criminal and terrorist use of cryptocurrencies

Criminals and terrorist are interested in cryptocurrencies as these technologies can challenge anti-money-laundering (AML) and counter terrorism financing (CTF) regimes. Indeed, their use lessens the reliance on financial intermediaries, increases the degree of anonymity and allows for near-instantaneous transactions.[46] Moreover, they can allow for circumventing geographical constraints and exploiting the gaps between different legislations.[47] In addition, when trading in cryptocurrencies on the Darknet, criminal and terrorist actors can increase the degree of anonymity by using the anonymising software *The Onion Router* (TOR), thus further challenging law enforcement investigative activities.[48] These factors attract the interests of both criminals and terrorists that see in cryptocurrencies an opportunity to avoid detection from law enforcement, while financing their activities.

[42] Fabian Maximilian Teichmann, "Current Trends in Terrorist Financing," *Journal of Financial Regulation and Compliance* 30, no. 1 (October 18, 2021): 107–25, https://doi.org/10.1108/jfrc-03-2021-0022.
[43] International Institute for Counter-Terrorism (ICT), "Cyber Report January-March 2021," *Www.ict.org.il* (International Institute for Counter-Terrorism (ICT), 2021), https://www.ict.org.il/Article/2708/CyberReportJanuaryMarch2021#gsc.tab=0.
[44] The Economist, "The Charm of Cryptocurrencies for White Supremacists," *The Economist*, February 5, 2022, https://www.economist.com/united-states/2022/02/05/the-charm-of-cryptocurrencies-for-white-supremacists.
[45] Southern Poverty Law Center (SPLC), "Cryptocurrency Report," Southern Poverty Law Center (SPLC), accessed March 8, 2022, https://www.splcenter.org/cryptocurrency-report.
[46] Anton Moiseienko and Kayla Izenman, "From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency" (Royal United Services Institute (RUSI), 2019), https://rusi.org/explore-our-research/publications/occasional-papers/intention-action-next-steps-preventing-criminal-abuse-cryptocurrency.
[47] Erik Silfversten et al., "Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes" (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR4418.html.
[48] Nikita Malik, "How Criminals and Terrorists Use Cryptocurrency: And How to Stop It," Forbes, 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/?sh=5a77c6039904.

Especially, terrorist organisations can find in cryptocurrencies means to support five main financing activities:[49]

1) *Fundraising* to support the organisation's activities.
2) *Illegal drug and arms trafficking* which can be a source of income for terrorist organisations.
3) *Remittance and transfer of funds* to meet the cash needs of the organisation.
4) *Attack funding* that includes weapons purchase and support to operational expenses.
5) *Operation funding* that concerns the broader set of the organisation's financial activities.

Each of these activities present core characteristics and requirements which can be fulfilled, to different degrees, by cryptocurrencies. For instance, cryptocurrencies' anonymity/pseudo-anonymity and security can facilitate the purchase of illegal drug and arms trafficking as well as the remittance and transfer of funds, attack funding and operation funding. Moreover, the user-friendly nature of cryptocurrencies and the high-speed of transactions can be pivotal to attack funding.

The most used cryptocurrencies by criminals and terrorists

BTC has been often associated with both criminal and terrorist activities. In a 2015 report, EUROPOL revealed that Bitcoin-related criminal activities accounted for 'for over 40% of all identified criminal-to-criminal payments.'[50] Although in 2018 it was still the most used cryptocurrency among criminals, other cryptocurrencies such as Monero, Litecoin and Dash have been used for illicit trading in Dark Web marketplaces.[51] However, both jihadi and far-right extremists are mainly advertising fundraising campaigns in BTC and XMR.[52] Although Bitcoin is the most preferred cryptocurrency due to its easy convertibility into fiat currencies, LTC can offer quicker transactions, while Monero presents higher degrees of anonymity.[53] An increase in the criminal use of Monero for both illicit purchases and ransomware extortion has been registered in recent years.[54]

While the above-mentioned cryptocurrencies have been connected to criminal and terrorist financing, there is still little evidence that other cryptocurrencies like Zcash are being used by

[49] Cynthia Dion-Schwarz, David Manheim, and Patrick B. Johnston, "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats" (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR3026.html.
[50] European Union Agency for Law Enforcement Cooperation (EUROPOL), *Internet Organised Crime Threat Assessment (IOCTA) : 2015* (The Hague: European Union Agency for Law Enforcement Cooperation (EUROPOL), 2015), https://www.europol.europa.eu/cms/sites/default/files/documents/europol_iocta_web_2015.pdf, 46.
[51] Anton Moiseienko and Olivier Kraf, "From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime" (Royal United Services Institute (RUSI), 2018), https://rusi.org/explore-our-research/publications/occasional-papers/money-mules-chain-hopping-targeting-finances-cybercrime.
[52] Shahed Warreth, "Crowdfunding and Cryptocurrency Use by Far-Right and Jihadi Groups," *VOX - Pol* (blog), November 21, 2019, https://www.voxpol.eu/crowdfunding-and-cryptocurrency-use-by-far-right-and-jihadi-groups/.
[53] Anton Moiseienko and Olivier Kraf, "From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime" (Royal United Services Institute (RUSI), 2018), https://rusi.org/explore-our-research/publications/occasional-papers/money-mules-chain-hopping-targeting-finances-cybercrime.
[54] Ibid.

criminals and terrorist groups.[55] However, the absence of evidence does not imply that these cryptocurrencies are not being used for illicit purposes. Indeed, Zcash presents characteristics facilitating money-laundering processes and has been mentioned on Jihadi-affiliated social media channels.[56] Furthermore, recent law enforcement investigations have showed a diversification in the cryptocurrencies hold by terrorist organisations. For instance, the Israeli government recently seized 84 wallets associated with Hamas, revealing that the organisation was trading in numerous cryptocurrencies, from Dogecoin and Cardano to Ripple and Ethereum.[57]

Barriers to the widespread criminal and terrorist use of cryptocurrencies

Although cryptocurrencies are being increasingly used by criminals and terrorists, they still constitute a small part of financial revenues and flows as the widespread adoption of these technologies is hindered by specific factors. Both cryptocurrencies' characteristics and law enforcement preparedness can create barriers to the criminal and terrorist use of cryptocurrencies.

The high volatility of prices and the potential inconvertibility of cryptocurrencies are major problems preventing the full-scale adoption of these technologies by criminals and terrorists.[58] Moreover, large transactions in cryptocurrencies are noticeable, thus attracting the attention of authorities.[59] Furthermore, the use of cryptocurrencies requires technological sophistication and can be constrained by the limited acceptance and usability of cryptocurrencies in the areas where terrorist groups operate.[60]

In addition, law enforcement and intelligence agencies' CTF measures and hackers' actions such as deanonymisation, spending denial, theft, and systemic attacks can negatively affect the criminal and terrorist use of cryptocurrencies.[61] Indeed, despite providing certain degrees of anonymity which, however, depend on the type of cryptocurrency, transactions leave traces, thus allowing for digital

---

[55] Sean Foley, Jonathan R. Karlsen, and Tālis J. Putniii, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?," *Review of Financial Studies* 32, no. 5 (2019): 1798–1853, https://doi.org/10.2139/ssrn.3102645; Erik Silfversten et al., "Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes" (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR4418.html.

[56] Gabriel Weimann, "Going Darker? The Challenge of Dark Net Terrorism" (Wilson Center, 2018), https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf; Chad Albrecht et al., "The Use of Cryptocurrencies in the Money Laundering Process," *Journal of Money Laundering Control* 22, no. 2 (May 7, 2019): 210–16, https://doi.org/10.1108/jmlc-12-2017-0074.

[57] Danny Nelson, "Israeli Seizure Order Shows Hamas Holds USDT, TRX, DOGE," *Www.coindesk.com* (blog), July 7, 2021, https://www.coindesk.com/policy/2021/07/07/israeli-seizure-order-shows-hamas-holds-usdt-trx-doge/.

[58] Alan Brill and Lonnie Keene, "Cryptocurrencies: The next Generation of Terrorist Financing?," *Defence against Terrorism Review* 6, no. 1 (January 15, 2014): 7–30, https://ssrn.com/abstract=2814914; Hannarae Lee and Kyung-Shick Choi, "Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework," *Victims & Offenders* 16, no. 3 (February 16, 2021): 363–84, https://doi.org/10.1080/15564886.2020.1835764.

[59] Cynthia Dion-Schwarz, David Manheim, and Patrick B. Johnston, "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats" (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR3026.html.

[60] Ibid.

[61] Ibid.

forensics analysis.[62] Especially, law enforcement agencies like the Federal Bureau of Investigation have developed advanced digital forensic capabilities, being able to connect cryptocurrencies' use to Internet Protocol (IP) addresses and arrest the individuals involved in the criminal use of cryptocurrencies.[63]

[62] Fabian Maximilian Teichmann, "Current Trends in Terrorist Financing," *Journal of Financial Regulation and Compliance* 30, no. 1 (October 18, 2021): 107–25, https://doi.org/10.1108/jfrc-03-2021-0022.

[63] John Bohannon, "Why Criminals Can't Hide behind Bitcoin," *Science*, March 9, 2016, https://doi.org/10.1126/science.aaf4167.

Bibliography

Albrecht, Chad, Kristopher McKay Duffin, Steven Hawkins, and Victor Manuel Morales Rocha. "The Use of Cryptocurrencies in the Money Laundering Process." *Journal of Money Laundering Control* 22, no. 2 (May 7, 2019): 210–16. https://doi.org/10.1108/jmlc-12-2017-0074.

Amarasinghe, Niluka, Xavier Boyen, and Matthew McKague. "A Survey of Anonymity of Cryptocurrencies." In *Proceedings of the Australasian Computer Science Week Multiconference*. Association for Computing Machinery, 2019. https://doi.org/10.1145/3290688.3290693.

Azani, Eitan, Michael Barak, Edan Landau, and Nadine Liv. "Identifying Money Transfers and Terror Finance Infrastructure." *Www.ict.org.il*. International Institute for Counter-Terrorism (ICT), 2020. https://www.ict.org.il/Article/2488/Identifying_Money_Transfers_and_Terror_Finance_Infrastructure#gsc.tab=0.

Baron, Joshua, Angela O'Mahony, David Manheim, and Cynthia Dion-Schwarz. *National Security Implications of Virtual Currency : Examining the Potential for Non-State Actor Deployment*. Santa Monica, Calif.: Rand National Defense Research Institute, 2015. https://www.rand.org/pubs/research_reports/RR1231.html.

BBC News. "Crypto Money Laundering Rises 30%, Report Finds." *BBC News*, January 26, 2022, sec. Technology. https://www.bbc.com/news/technology-60072195.

———. "Squid Game Crypto Token Collapses in Apparent Scam." *BBC News*, November 2, 2021, sec. Business. https://www.bbc.com/news/business-59129466.

Bloomberg, Jason. "Using Bitcoin or Other Cryptocurrency to Commit Crimes? Law Enforcement Is onto You." *Forbes*, 2017. https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/?sh=7cf28343bdc4.

Boge, Ariel. "How Australia's Far Right Uses Cryptocurrencies to Monetise Hate Online." *The Guardian*, December 27, 2021. https://www.theguardian.com/technology/2021/dec/28/how-australias-far-right-uses-cryptocurrencies-to-monetise-hate-online.

Bohannon, John. "Why Criminals Can't Hide behind Bitcoin." *Science*, March 9, 2016. https://doi.org/10.1126/science.aaf4167.

Brill, Alan, and Lonnie Keene. "Cryptocurrencies: The next Generation of Terrorist Financing?" *Defence against Terrorism Review* 6, no. 1 (January 15, 2014): 7–30. https://ssrn.com/abstract=2814914.

Brown, Steven David. "Cryptocurrency and Criminality." *The Police Journal: Theory, Practice and Principles* 89, no. 4 (August 3, 2016): 327–39. https://doi.org/10.1177/0032258x16658927.

Butler, Simon. "Criminal Use of Cryptocurrencies: A Great New Threat or Is Cash Still King?" *Journal of Cyber Policy* 4, no. 3 (September 2, 2019): 326–45. https://doi.org/10.1080/23738871.2019.1680720.

Carlisle, David. “Cryptocurrencies and Terrorist Financing: A Risk, but Hold the Panic.” *Rusi.org* (blog), 2017. https://rusi.org/explore-our-research/publications/commentary/cryptocurrencies-and-terrorist-financing-risk-hold-panic.

———. “Virtual Currencies and Financial Crime: Challenges and Opportunities.” Royal United Services Institute (RUSI), 2017. https://rusi.org/explore-our-research/publications/occasional-papers/virtual-currencies-and-financial-crime-challenges-and-opportunities.

Chavez-dreyfuss, Gertrude. “Cryptocurrency Crime in 2021 Hits All-Time High in Value - Chainalysis.” *Reuters*, January 6, 2022, sec. U.S. Markets. https://www.reuters.com/markets/us/cryptocurrency-crime-2021-hits-all-time-high-value-chainalysis-2022-01-06/.

Department of Justice. “AlphaBay, the Largest Online ‘Dark Market,’ Shut Down.” *Www.justice.gov*, July 20, 2017. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

———. “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns.” *Www.justice.gov*, August 12, 2020. https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

Di Cori, Arianna. “Gli Hacker Bloccano I Vaccini in Tilt Il Portale Del Lazio: ‘Pagate Il Riscatto in Bitcoin.’” *La Repubblica*, August 2, 2021. https://www.repubblica.it/cronaca/2021/08/02/news/gli_hacker_bloccano_i_vaccini_in_tilt_il_portale_del_lazio_pagate_il_riscatto_in_bitcoin_-312647208/.

Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston. “Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats.” Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3026.html.

European Cybercrime Center (EC3). “Police Ransomware Threat Assessment,” 2014. https://www.europol.europa.eu/cms/sites/default/files/documents/policeransomware-threatassessment.pdf.

European Union Agency for Law Enforcement Cooperation (EUROPOL). “Cryptocurrencies - Tracing the Evolution of Criminal Finances.” Luxembourg: Publications Office of the European Union, 2021. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf.

———. *Internet Organised Crime Threat Assessment (IOCTA) : 2015*. The Hague: European Union Agency for Law Enforcement Cooperation (EUROPOL), 2015. https://www.europol.europa.eu/cms/sites/default/files/documents/europol_iocta_web_2015.pdf.

Financial Action Task Force (FATF). “Virtual Currencies - Key Definitions and Potential AML/CFT Risks.” Financial Action Task Force (FATF), 2014. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

Fletcher, Emily, Charles Larkin, and Shaen Corbet. “Countering Money Laundering and Terrorist Financing: A Case for Bitcoin Regulation.” *Research in International Business and Finance* 56 (January 2021): 1–16. https://doi.org/10.1016/j.ribaf.2021.101387.

Fletcher, Emma. “Cryptocurrency Buzz Drives Record Investment Scam Losses.” *Federal Trade Commission (FTC)* (blog), May 17, 2021. https://www.ftc.gov/news-events/blogs/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses.

Foley, Sean, Jonathan R. Karlsen, and Tālis J. Putniii. “Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?” *Review of Financial Studies* 32, no. 5 (2019): 1798–1853. https://doi.org/10.2139/ssrn.3102645.

Greenberg, Andy. “Agora, the Dark Web’s Biggest Drug Market, Is Going Offline.” *Wired*, 2015. https://www.wired.com/2015/08/agora-dark-webs-biggest-drug-market-going-offline/.

Houben, Robby, and Alexander Snyers. “Cryptocurrencies and Blockchain.” Policy Department for Economic, Scientific and Quality of Life Policies, 2018. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.

Hunt, John. “The New Frontier of Money Laundering: How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and How Governments Are Trying to Stop Them.” *Information & Communications Technology Law* 20, no. 2 (June 2011): 133–52. https://doi.org/10.1080/13600834.2011.578933.

International Institute for Counter-Terrorism (ICT). “Cyber Report January-March 2021.” *Www.ict.org.il*. International Institute for Counter-Terrorism (ICT), 2021. https://www.ict.org.il/Article/2708/CyberReportJanuaryMarch2021#gsc.tab=0.

Izenman, Kayla, and Rick McDonell. “RUSI-ACAMS Cryptocurrency Risk & Compliance Survey.” Royal United Services Institute (RUSI); Association of Certified Anti-Money Laundering Specialists (ACAMS), 2020. https://www.acams.org/en/ACAMS-RUSI-Crypto-Survey-Report.

Keatinge, Tom, David Carlisle, and Florence Keen. “Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses.” Policy Department for Citizens’ Rights and Constitutional Affairs, 2018. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

Kethineni, Sesha, and Ying Cao. “The Rise in Popularity of Cryptocurrency and Associated Criminal Activity.” *International Criminal Justice Review* 30, no. 3 (February 6, 2019): 325–44. https://doi.org/10.1177/1057567719827051.

Kshetri, Nir, and Jeffrey Voas. “Do Crypto-Currencies Fuel Ransomware?” *IT Professional* 19, no. 5 (2017): 11–15. https://doi.org/10.1109/mitp.2017.3680961.

Lee, Hannarae, and Kyung-Shick Choi. “Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework.” *Victims & Offenders* 16, no. 3 (February 16, 2021): 363–84. https://doi.org/10.1080/15564886.2020.1835764.

Liv, Nadine. “Jihadists Use of Virtual Currency 2.” *Www.ict.org.il*. International Institute for Counter-Terrorism (ICT), 2019. https://www.ict.org.il/Article/2413/Jihadists_Use_of_Virtual_Currency_2#gsc.tab=0.

Malik, Nikita. “How Criminals and Terrorists Use Cryptocurrency: And How to Stop It.” Forbes, 2018. https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/?sh=5a77c6039904.

Moiseienko, Anton, and Kayla Izenman. “From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency.” Royal United Services Institute (RUSI), 2019. https://rusi.org/explore-our-research/publications/occasional-papers/intention-action-next-steps-preventing-criminal-abuse-cryptocurrency.

Moiseienko, Anton, and Olivier Kraf. “From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime.” Royal United Services Institute (RUSI), 2018. https://rusi.org/explore-our-research/publications/occasional-papers/money-mules-chain-hopping-targeting-finances-cybercrime.

Nelson, Danny. “Israeli Seizure Order Shows Hamas Holds USDT, TRX, DOGE.” *Www.coindesk.com* (blog), July 7, 2021. https://www.coindesk.com/policy/2021/07/07/israeli-seizure-order-shows-hamas-holds-usdt-trx-doge/.

Noonan, Laura. “Ireland Defies Hackers’ Bitcoin Demand over Health System.” *Financial Times*. May 14, 2021. https://www.ft.com/content/ed8d3643-1966-45b5-a31c-28dcaf93a65a.

Oré, Diego. “Latin American Crime Cartels Turn to Cryptocurrencies for Money Laundering.” *Reuters*, December 8, 2020. https://www.reuters.com/article/mexico-bitcoin-insight-idUSKBN28I1KD.

Patel, Pankaj C., and Igor Pereira. “The Relationship between Terrorist Attacks and Cryptocurrency Returns.” *Applied Economics* 53, no. 8 (October 4, 2020): 1–22. https://doi.org/10.1080/00036846.2020.1819952.

Rodeck, David, and John Schmidt. “What Is Blockchain?” *Forbes Advisor*, June 9, 2021. https://www.forbes.com/advisor/investing/what-is-blockchain/.

Seele, Peter. “Let Us Not Forget: Crypto Means Secret. Cryptocurrencies as Enabler of Unethical and Illegal Business and the Question of Regulation.” *Humanistic Management Journal* 3, no. 1 (May 30, 2018): 133–39. https://doi.org/10.1007/s41463-018-0038-x.

Silfversten, Erik, Marina Favaro, Linda Slapakova, Sascha Ishikawa, James Liu, and Adrian Salas. “Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes.” Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR4418.html.

Southern Poverty Law Center (SPLC). “Cryptocurrency Report.” Southern Poverty Law Center (SPLC). Accessed March 8, 2022. https://www.splcenter.org/cryptocurrency-report.

Teichmann, Fabian Maximilian. “Current Trends in Terrorist Financing.” *Journal of Financial Regulation and Compliance* 30, no. 1 (October 18, 2021): 107–25. https://doi.org/10.1108/jfrc-03-2021-0022.

The Economist. “The Charm of Cryptocurrencies for White Supremacists.” *The Economist*, February 5, 2022. https://www.economist.com/united-states/2022/02/05/the-charm-of-cryptocurrencies-for-white-supremacists.

The Soufan Center. “IntelBrief: Terrorists’ Use of Cryptocurrency.” The Soufan Center, December 10, 2020. https://thesoufancenter.org/intelbrief-2020-december-10/.

Trautman, Lawrence J. “Virtual Currencies: Bitcoin & What Now after Liberty Reserve and Silk Road?” *Richmond Journal of Law & Technology* XX, no. 4 (2014). https://doi.org/10.2139/ssrn.2393537.

United Nations Office on Drugs and Crime (UNODC). *World Drug Report 2018*. United Nations Office on Drugs and Crime (UNODC), 2018.

Vidino, Lorenzo, Jon Lewis, and Andrew Mines. “Dollars for Daesh: The Small Financial Footprint of the Islamic State’s American Supporters – Combating Terrorism Center at West Point.” *CTC Sentinel* 13, no. 3 (March 24, 2020): 24–29. https://ctc.westpoint.edu/dollars-daesh-small-financial-footprint-islamic-states-american-supporters/.

Warreth, Shahed. “Crowdfunding and Cryptocurrency Use by Far-Right and Jihadi Groups.” *VOX - Pol* (blog), November 21, 2019. https://www.voxpol.eu/crowdfunding-and-cryptocurrency-use-by-far-right-and-jihadi-groups/.

Weimann, Gabriel. “Going Darker? The Challenge of Dark Net Terrorism.” Wilson Center, 2018. https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf.

Whyte, Christopher. “Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise.” *Studies in Conflict & Terrorism*, January 2, 2019, 1–24. https://doi.org/10.1080/1057610x.2018.1531565.

Woolf, Nicky. “Bitcoin ‘Exit Scam’: Deep-Web Market Operators Disappear with $12m.” *The Guardian*, March 18, 2015. https://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars.

Centar za sigurnosne studije - BIH

Centre for Security Studies - BH

BOSNA I HERCEGOVINA
71000 SARAJEVO
BRANILACA SARAJEVA 13/1

TEL:
+ 387 (0)33 262-456

info(at)css.ba

@CSSBIH

www.css.ba