Think Visegrad
V4 Think-Tank Platform

October 2021

Policy Paper

Terrorism, Cryptocurrencies, and the EU Response

Asya Metodieva

October
2021

Contents

Abstract

Cryptocurrencies have created space for terrorists, extremists, and other criminal actors to support their activities through unregulated anonymous transactions. While the exchange of crypto assets is not the primary financial channel of established terrorist organizations, mid- and small-scale networks increasingly rely on it. The new technology is gaining recognition in more and more countries but lacks sufficient regulation to curb illicit activities. This gap provides terrorists with means to transfer financial information, fundraise, and store financial resources anonymously. The regulation of cryptocurrencies is under discussion at EU level, and a new regulatory framework was announced earlier in 2021. The proposed changes would force companies that transfer crypto assets to collect details on the recipient and sender. Currently, not all national Financial Intelligence Units (FIUs) have the capacity to track suspicious crypto transactions and uneven regulations across EU members create the risk that any differences could be exploited by terrorists and other actors who pursue illicit activities. This policy paper discusses what terrorists use cryptocurrencies for. It further assesses the ongoing regulatory initiatives at the EU level. Finally, it looks at how the Visegrad Four (V4) countries, and Czechia more specifically, approach crypto transfers in relation to terrorism-related threats at the national level. This study is the outcome of expert interviews and desk research of documents conducted in Brussels in July-August 2021. It is the result of a cooperation between Europeum Institute for European Policy and the Institute of International Relations Prague.

October 2021

Recommendations

- The V4 countries should increase the cooperation between the national Financial Intelligence Units (FIUs) in the region to address challenges related to the cross-border nature of cryptocurrencies.
- The V4 countries are advised to build the capacity to regulate or track crypto-to-crypto transactions. While the current EU framework deals only with crypto-to-fiat exchanges, the member states need to invest in better tracking of crypto-to-crypto transactions potentially linked to terrorism.
- The V4 countries are advised to analyse the risks posed by privacy coins, non-custodial wallets, and exchanges with enhanced protection of users' data.

October 2021

Introduction

Terrorists have proved to be particularly creative in adopting new technologies for communication, propaganda, or to finance their activities. There are two features that make cryptocurrencies appealing to such actors: first, the technology itself preserves anonymity; second, it is handy, as it is accessible through smartphones, thus, gives users an immediate access to their crypto wallets.[1] Terrorists have widely embraced these features, but the technology is used differently depending on the financial structure, the goals, and the size of a terrorist organization. Large-size groups rely on a variety of revenue sources, whereas support networks and lone-wolf-inspired terrorists are more dependent on monetary assets. Terrorists further need support that is not always related to terrorist attacks but that can reduce costs and make financial resources available for other activities, such as propaganda or recruitment. [2] The cost of attacks has changed dramatically in the recent years, consequently, the financing of terrorism has changed as well.[3] From the 9/11 attacks and the 2005 London bombings, for which there was costal planning and carrying out, today's terrorist assaults are more often self-funded. Jihadi terrorist attacks in Western Europe have generally been cheaper in the recent years, with three quarters of the plots estimated to cost less than $10,000.[4] Thus, for financing small-scale attacks, crypto transfers are an ideal tool. More importantly, they play a role in sustaining networks and maintaining propaganda campaigns.[5]

[1] Interviewee 1: Maria Demertzis, a Deputy Director at Bruegel, Online, Date: 15/07/2021.
[2] The Financial Action Task Force (FATF), Report, October 2013, 'Terrorist Financing in West Africa', accessed 19/09/2021.
[3] Global Terrorism Index 2017. Measuring and Understanding the Impact of Terrorism. Accessed 4/9/2021.
[4] Interviewee 2: Counter Terrorism Policy Officer, the European Commission, In Person, 19/07/2021.
[5] Ibid.

The Financing of Terrorism and Cryptocurrencies

There are several methods of financing used by terrorist actors most frequently: informal transfers (hawala), cash couriers, formal bank transfers, false trade invoicing, money service business (such as Western Union), and high value commodities.[6] The reliance on different streams of revenue is regardless of an ideology: both right-wing and jihadi terrorists rely on variety of sources, including drug dealing, selling weapons, donations, etc. (See Table 1.). Jihadists are more advanced in embracing the use of cryptocurrencies, as jihadi activism is rooted in transnational networks that requires fast anonymous transfers overcoming national borders. Right-wing financial supporters, on the other hand, have adopted a more localized approach, and they are often located in the same geographical areas where activities are planned.[7]

Table 1. Income Sources of European Jihadi Cells.[8]

Salaries and savings of network members	More than 70% from legal sources
Illegal trade in drugs, weapons, and other goods	Around 30% from criminal activities
Theft and Robbery	Around 50% of the cells are self-financed

The use of online payment systems (such as PayPal, Swish, etc.) and cryptocurrencies is the most recent addition to this list. Although cryptocurrencies are not the key financing tool used by terrorists, the technology offers advantages for individuals and groups to engage in illicit behaviour. [9] Making transactions anonymous guarantees that the identity of an user is encrypted, and while the wallet is publicly visible, the user's personal

[6] Freeman, Michael and Ruehsen, Moyara. 2013. 'Terrorism Financing Methods: An Overview', Perspectives on Terrorism, Vol. 7, Issue 4. Accessed 17/09/2021.
[7] Interviewee 2.
[8] Oftedal Emilie. 2015. 'The Financing of Jihadi Terrorist Cells in Europe', Norwegian Defence Research Establishment (FFI), 9/1/2015. Accessed 8/8/2021.
[9] Schindler, Hans-Jakob, Hanley-Giersch, Jennifer, Eisermann, Daniel. 2020. 'Further development of European Union Regulatory Framework for Cryptocurrencies necessary to mitigate Risks of Terrorism Financing'. Counter Extremism Project (CEP) and Berlin Risk. Accessed 12/9/2021.

identification data is not.[10] Transactions are publicly recorded on the blockchain, but the concept of anonymity secures individual users' privacy. [11] Keeping the identity of cryptocurrency users confidential is a major challenge for security experts countering terrorist financing. What makes cryptocurrencies even more appealing to terrorist actors is the involvement of *tumblers* and *mixers* [12] that break up individual transactions and re-assemble them in a different form. *Mixers* and *tumblers* combine the cryptocurrency of one transaction with those of others before sending the correct amount to the receiver, thus masking the path of a transaction and further reducing the knowledge about the link between a user and a receiver. [13] As terrorism financing in Europe usually involves small sums to finance cells or individual attacks, not knowing the identity of senders and receivers, as well as their potential ties to a terrorist group, makes the prevention of terrorism financing very challenging.[14]

There are four main ways, in which terrorists use cryptocurrencies: to raise funds, as an alternative payment method, to store and send funds securely, to camouflage criminal behavior.[15]

Raise funds: Cryptocurrencies provide terrorists with much freedom in asking for donations to raise funds. While actors across various ideological spectra rely on crowdfunding platforms to raise funds, jihadists have gained more experience than right-wing actors in using this approach. For instance, social media pages and accounts have added the possibility for crypto transfers to support the IS females currently kept in the al-Hol camp in Syria.[16]

The usual practice involves an individual linked to a particular group who announces their crypto account publicly and asks targeted groups online to make transfers.

[10] BitDegree. 2020. 'Anonymous Bitcoin Wallet and How to Get Bitcoins Anonymously'.
[11] Schindler, Hanley-Giersch, and Eisermann 2020.
[12] Eurospider. 2020. 'What is a cryptocurrency mixer?'
[13] Schindler, Hans-Jakob. 2020. 'Misuse of online services for the financing of terrorism', Counter Extremism Project (CEP).
[14] Schindler, Hanley-Giersch, and Eisermann 2020.
[15] Interviewee 3: Hans-Jakob Schindler, Senior Director of the Counter Extremism Project, Online, 27/07/2021.
[16] Beck John, 'Funding the Needy, or Funding Terror?', Rest of The World, 21/02/2021, Accessed: 10/08/2021.

Donations may vary from 10 EUR to half a million EUR, according to data from European counterterrorism agencies. [17] Even if the recipient can be identified but is not classified as a member of a terrorist organization, this makes it difficult to prosecute them.[18]

> 'For every person that is ready to travel abroad as a foreign terrorist fighter as a result of a radicalization campaign, there will be a larger number of supporters and potential financiers who will say, well, I cannot go to Syria with my family, but my contribution to jihad will be a financial one. So, there is a direct link with recruitment of fighters and an increasing the number of donations.'[19]

The fundraising platforms are mainly Bitcoin-oriented, perhaps because it is easy to cash out from crypto to fiat currencies. Meanwhile, terrorists have made several innovations.[20] What can be called a crypto migration is caused by the realization of terrorist actors that they are already at risk when using established platforms for crypto exchange. One example is the Palestinian organization Hamas that previously had a cryptocurrency drive on a wallet at Coinbase, [21] which is a regulated US exchange. Understanding that if they use a transparent platform, they will inevitably run into the risk of getting their money blocked, the group moved their crypto activities to another jurisdiction.[22] Another innovation is the use of a unique QR code for each transaction.[23] Every time when a user clicks on the same QR code, they get a different wallet address. The creation of a unique QR code means that an investigative agency would have to actually donate to a terrorist group to find out one of the many wallet addresses that a group or an individual of interest seem to be using.[24] The difference between how right-wing and Islamist extremists use cryptocurrencies is in the need for obfuscation. [25] In many jurisdictions, it is very risky for an IS financier or a supporter of Hamas or Hezbollah, for instance, to donate money. Thus, such actors look for ways to obfuscate their financial activities. On the contrary,

[17] Interviewee 2.
[18] Ibid.
[19] Ibid.
[20] Interviewee 3.
[21] Coinbase.
[22] Wilson, Tom, and Williams, Dan, 'Hamas shifts tactics in bitcoin fundraising, highlighting crypto risks: research' , Reuters, 26/4/2019. Accessed 19/9/2021.
[23] Interviewee 3.
[24] Ibid.
[25] Ibid.

right-wing extremists enjoy more freedom because the organizations that they are affiliated with are not designated as terrorist. Right-wing extremists ask for donations in crypto, but it is not done out of absolute necessity like in the case of IS.[26]

An alternative payment method: Terrorists increasingly use cryptocurrencies as an alternative payment method, as many individuals linked to terrorist networks are banned from opening a bank account. Although right-wing actors in the broader radical milieu still rely on bank transactions, they also get income from online sales, for example from selling t-shirts online.[27] As big payment providers (such as Visa and Mastercard) seek to protect their own reputation and refuse services to right-wing platforms, extremists migrate to new payment methods, such as cryptocurrencies, which appear to be an easy and accessible alternative. According to a 2021 report by Europol, the number of cases involving the misuse of new payment methods, especially cryptocurrencies, remained low in 2020.[28] Nonetheless, the potential to use them to finance terrorism, has been evident on several occasions both in Europe and the U.S. Among others, Nordisk Styrka (NS, 'Nordic Strength') and Nordfront, the Nordiska motståndsrörelsen (NMR, 'Nordic Resistance Movement') call on their followers to donate Bitcoin via different websites. These organizations have had their bank accounts terminated by Swedish banks and, therefore, have the only option of receiving donations in cryptocurrencies.[29]

To store and send funds securely: Terrorists find particularly beneficial the uneven regulatory regimes across countries, so they can make crypto transfers, which in many cases remain untracked. At the moment, terrorists can move their financial activities to countries where there is a more flexible regulation or no regulation at all. Considering this a security threat, the U.S. and the EU seek to build a resilient regulatory framework regarding cryptocurrencies. In August 2020, the U.S.

[26] Interviewee 3.
[27] Kacper Rekawek, Alexander Ritzmann, Hans Jakob Schindler, 'Violent Right-Wing Extremism and Terrorism. Transnational Connectivity, Definitions, Incidents, Structures and Countermeasures', CEP 2020. Accessed 8/9/2021.
[28] Europol, 'European Union Terrorism Situation and Trend Report 2021 (TESAT)', 22/6/2021. Accessed 12/10/2021.
[29] Ibid.

Department of Justice announced the seizure of more than 300 cryptocurrency accounts following the suspicion that they were used for terrorist financing campaigns of groups linked to the Islamic State (IS) and Al Qaeda, as well as Qassam Brigades, Hamas's military wing. [30] The accounts amounted the equivalent of several million US dollars.

Meanwhile, the EU does not have the mechanisms to seize such transactions, neither to freeze crypto wallets, if an individual or a group maintain such funds in another jurisdiction where different rules are applied.[31]

To obfuscate criminal behavior: Looking at the demand side of what terrorist organizations accept as payments, the use of privacy coins has increased over the last two years, as this is a safer version of cryptocurrencies, if one intends to hide criminal behaviour.[32] If an organization has money laundering activities and seeks to make this less obvious, it can use crypto to obfuscate the transactions.[33] In a recent case, funds were obtained through a bank fraud and laundered through crypto transfers and, eventually, an attempt was made to send the amount to a terrorist group.[34]

While terrorist actors use Bitcoin as it is the most widely recognized cryptocurrency, their interest in the so-called privacy coins[35] is also increasing. Privacy coins are particularly appealing due to their enhanced encryption of both individual wallets and a user's identity. [36] For instance, online platforms linked to right-wing extremists accept privacy coins such as Monero. [37] Similarly, jihadi groups promote exchange and services in privacy coins, among them is the group Hayat Tahrir al Sham (HTS) active in Syria.[38] Stablecoins[39] could also

[30] The United States Department of Justice, 'Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts' 13/8/2020. Accessed 13/10/2021.
[31] Interviewee 3.
[32] Ibid.
[33] Ibid.
[34] Department of Justice, U.S. Attorney's Office, Eastern District of New York, 'Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists' 14/12/2017. Accessed 14/9/2021.
[35] Vermaak Werner, 2021, 'What are Privacy Coins', 7/4/2021. Accessed 29/9/2021.
[36] Eisermann Daniel. 2020. 'Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory, Challenges', Berlin Risk/Counter Extremism Project.' Accessed 18/9/2021.
[37] Monero website
[38] Rekawek Kacper, Ritzmann Alexander, Schindler Hans Jakob. 2020.
[39] Stablecoins.

attract the attention of terrorist users, especially of those linked to large-scale organizations, because stablecoins solve the issue of volatility and link the new currency to a basket of assets that is known to be stable (could be linked to EUR or US dollar). People interested in illicit activities on a large scale can benefit from stablecoins because this variant of cryptocurrencies gives certainty in the value of transactions. [40] Libra, the stablecoin previously introduced by Facebook, could become massive in use, since the social media platform has access to billions of users, but their stablecoin project did not survive a backlash from the EU.[41]

Regulation of Cryptocurrencies in the EU

In 2021, the Financial Action Task Force (FATF) released new guidance recommending that regulators should identify mixers, tumblers, and other instruments that seek to make crypto transactions less transparent. [42] The guidance also pays attention to the risks posed by variations in the regulatory framework across countries. This gap is already exploited by terrorist actors who have the interest to move their crypto activities from more to less regulated jurisdictions.[43]

In July 2021, The European Commission presented an ambitious package of legislative proposals to enhance the EU's anti-money laundering and countering the financing of terrorism (AML/CFT) standards. The package harmonizes AML/CFT rules across the EU and further proposes the creation of a new EU agency to fight money laundering.[44] The new EU authority is expected to enhance the cooperation among national financial intelligence units (FIUs). The European Commission has started to move forward in

[40] Interviewee 1.
[41] Valero, Jorge, 23/6/2020. 'Commission to present 'strong' rules for Facebook's Libra'. Accessed 20/9/2021. https://www.euractiv.com/section/economy-jobs/news/commission-to-present-strong-rules-for-facebooks-libra/

[42] FATF, Draft updated Guidance for a risk-based approach to virtual assets and VASPs, 2021, 16.
[43] Schindler, 'Misuse of online services for the financing of terrorism'.
[44] 'Anti-money laundering and countering the financing of terrorism legislative package', European Commission. Accessed 9/8/2021.

2020 with an Action plan,[45] which seeks to regulate crypto assets and provide the possibility for member states to recognize cryptocurrencies as a part of the financial markets. The new framework builds on the 5th Money Laundering Directive (AMLD5) [46] where cryptocurrencies were involved for the first time. Previously, the focus was on regulating the crypto-to-fiat transactions, but there is an increasing need to also regulate crypto-to-crypto exchanges.

> 'This technological innovation has a lot of merit, it uses blockchain technology, which allows to send value in a safe way. Through the blockchain, [one] can guarantee certain invariability of the transaction. It provides a level of safety that it did not exist before, the transactions are also verified by a network of controllers. However, the more worrying side is that this technology also allows anonymity. And the risk is that these virtual currencies are used in an anonymous way to perpetrate crimes or to launder money linked to criminal activities.'[47]

The new regulatory efforts include a comprehensive new legislative proposal on crypto assets, called Markets in Crypto-assets (MiCA)[48] that was developed to help streamline distributed ledger technology (DLT) and virtual asset regulation, whilst protecting users and investors. MiCA, developed since 2018, promises to regulate currently out-of-scope crypto-asset types such as stablecoins, as well as crypto-asset service providers.[49] The Commission seeks to create a framework guaranteeing that crypto exchanges in all member states is safe, yet this process is not entirely in the hands of Brussels.

> 'We do not know who the issuer [of Bitcoin] is. It is very difficult to have credibility if we do not know who the issuer [of the most popular cryptocurrency] is. [Additionally], the issuer [shows] no interest in the monetary policy. The supply of Bitcoins is what it is, it is a line that goes to an end around 100 years from now. By construction, it is an algorithm and therefore, if the demand goes up by a lot

[45] 'Action plan for a comprehensive Union policy on preventing money laundering and terrorism financing', European Commission.7/5/2020. Accessed 12/8/2021.
[46] Anti-money laundering (AMLD V) - Directive (EU) 2018/843
[47] Interviewee 4: A source from the Directorate-General for Financial Stability, Financial Services and Capital Markets Union, DG FISMA at the European Commission, Online, 28/9/2021.
[48] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, The European Commission, Brussels, 24.9.2020, COM (2020) 593 final, 2020/0265(COD).
[49] 'MiCA: A Guide to the EU's Proposed Markets in Crypto-Assets Regulation'

> and the supply is not adjusting, the price will go up. There is no management of the currency, and thus, it is volatile.'[50]

The crypto-to-crypto transactions are expected to be regulated through MiCA, but meanwhile, privacy coins, tumbles, and mixers, as well as non-custodial wallets exchange are rapidly developing the past two years. These tools allow pure peer-to-peer transactions without the provision of an intermediary. [51] The proposal of the European Commission concerning cryptocurrencies may take up to four years to be formally adopted in the EU legislation. Additionally, MiCA promises to control crypto exchanges but only within the EU, which raises criticisms:

> 'Imagine that you have an extortion on the basis of a crypto network, and someone tells you: look, I will reveal these photos of you unless you pay this amount of money somewhere outside the EU. In this case, the EU does not have the mechanism to investigate and prosecute this network because they will not know where the crypto receiver is based'.[52]

Currently, some European countries are more flexible in how they treat cryptocurrencies, (among them are Switzerland, Spain, Malta), whereas others are very reluctant. It is likely that differences among member states will remain significant in the coming years until the new EU legislation is adopted. Additionally, the general EU regulation could be a challenge because checking the transactions of regular consumers contradicts the increased protection of customer data. Despite current regulatory efforts, it is likely that the technology behind cryptocurrencies is resilient enough to prevent exposing the anonymity of users. This is so because it is hard to track every single user who generates their individual cryptocurrency wallets using cryptographic technics directly on their own computers.[53] Consequently, only a new generation of monitoring tools that enable authorities to decipher privacy coin transactions may help mitigate the risks related to terrorism

[50] Interviewee 1.
[51] Schindler, Hanley-Giersch, and Eisermann 2020.
[52] Interviewee 5: Karel Lannoo, Chief Executive of The Centre for European Policy Studies (CEPS), Online, Date: 19/7/2021.
[53] Interviewee 6: Mikulas Peksa, a Member of the European Parliament from Greens–European Free Alliance, a member of the Czech Pirate Party, Online, 7/9/2021.

financing. [54] A blockchain analysis is a possible solution that can provide information and be useful to identify users linked to terrorist groups. It is a statistical analysis of transactions that has not been used as evidence in court cases yet. The statical data gives information about the transaction flows but there is no proof that a wallet actually belongs to a particular individual. Thus, security analysts seek to find enough indicators or look for a mistake of some of the participants in the transaction process that can lead to the suspect. This type of investigation is applicable to Bitcoin, yet, tracing the process of privacy coins transactions such as Monero or Ethereum is close to impossible at the moment.[55]

To sum up, there are three major weaknesses of the EU approach at the moment: 1) It does not have power over crypto exchanges done outside of the EU jurisdiction; 2) It does not deal with privacy coins, tumblers, mixers, non-custodial wallets exchanges. While these tools represent a serious regulatory challenge, they are also an opportunity for terrorists and the financing of illicit activities more generally; 3) National FIUs across the EU have uneven expertise and resources to track, report, and investigate suspicious crypto transactions. At the national level, member states have their FIUs in charge of receiving suspicious transaction reports. Upon their request, existing financial institutions are obliged to not execute a particular transaction if the FIU finds it suspicious of potential money laundering or financing of terrorism. While all these actions are part of member states' jurisdictions, crypto activities are transnational and require enhanced international cooperation. The European Commission's proposal to create a European financial intelligence agency can be a mechanism to increase cooperation between FIUs at the national level.[56]

The Visegrad Four, Crypto Regulation and the Terrorist Threat

The Visegrad states assess the overall threat of terrorism from low to medium levels.[57]

[54] Schindler, Hans-Jakob, Hanley-Giersch, Jennifer, Eisermann, Daniel. 2020, 9.
[55] Interviewee 3.
[56] Interviewee 4.
[57] Czechia: medium; Poland: low; Slovakia: increased; Hungary: medium. Source: Globsec, 'Report 1 Visegrad Four: Countering the financing of

Although countries of the region have included the priority to counter terrorism financing in their strategic documents, the issue of crypto regulation is not tied to the concept of national security in this particular aspect. National FIUs that deal with terrorism financing are embedded in different parts of national institutional infrastructures[58] and this may prevent their efficient cooperation in some cases. For instance, The Hungarian FIU is located within the organisation of the Central Management of the National Tax and Customs Administration, under the Ministry of Finance.[59] The Polish FIU "The General Inspector of Financial Information – GIFI" is located in the Ministry of Finance, with the main authority for combating money laundering and financing terrorism. [60] In Czechia, the Financial Analytical UNIT (FAU) deals with financial intelligence regarding illicit activities and along with the coordinator of the National Risk Assessment process (NRA) provides the analysis and transmission of suspicious reports regarding money laundering/combating the financing of terrorism (AML/CFT).[61] Slovakia's FIU is the only one in the region placed in the Ministry of Interior. The small number of investigations into terrorism financing (three at the moment) emphasizes the low threat Slovakia faces. Among the potential risks for the country are poor control of the cash movements across the country; money remittances, the use of fictitious corporate structures; non-dissuasive nature of sanctions in relation to undeclared/falsely declared movement of cash.[62]

In February 2021, the V4 countries signed a joint declaration on cooperation in digital affairs. [63] While the declaration promises cooperation in developing new products,

terrorism while not directly threatened by terrorism', 25/5/2021. Accessed 4/8/2021.

[58] Globsec, 'Report 1 Visegrad Four: Countering the financing of terrorism while not directly threatened by terrorism', 25/5/2021. Accessed 4/8/2021.

[59] Ibid.

[60] Ibid.

[61] Moneyval, 'Anti-Money Laundering and Counter-Terrorist Financing Measures - Czech Republic, Fifth Round Mutual Evaluation Report,' December 2018. Accessed 8/8/2021, [61] Globsec, 'Report 1 Visegrad Four: Countering the financing of terrorism while not directly threatened by terrorism'.

[62] Ibid.

[63] Visegrad Group Joint Declaration on Mutual Co-operation in Digital Projects, Krakow, February 17, 2021.

business models, investments, or research in the field of digital transformation, including artificial intelligence (AI), machine learning, blockchain, cybersecurity and telecommunication, companies across the region lag behind in the integration of new technologies and do not have a clear vision in terms of their digital transformation.[64] At the same time, companies across the region are seen as international leaders in cybersecurity.[65] The Czech capital is ranked one of the most crypto-friendly cities in the world, as in many cases goods and services can be purchased via crypto transactions.[66] Some parties, like the Czech Pirate Party, are in favor of involving crypto currencies into the financial system, instead of overregulating them:

> 'We may criticize [the technology] but this is the way cryptography works: it provides you a certain degree of anonymity and decentralization. For people who seek financial anonymity for some reason, they are a logical tool to choose. Some people have legitimate purposes, for instance, dissidents in Iran, in occupied Crimea. And there are people who use crypto for illegitimate reasons. At the end of the day, [crypto] is a tool. You can use a knife to cut your bread, or to kill people.'[67]

The threat of terrorism to Czechia is assessed as 'medium', as the country has not experienced major terrorist attacks and only few cases of radicalisation in the recent years.[68] Concerning the financial aspect of the threat, The National Risk Assessment (NRA) notes the following key areas as risks: transfer of funds for the purpose of financing of terrorism (FT) through cash couriers; corruption in both the public and private sectors; insufficient criminalization of the FT offence, among others. [69] The Czech legislator has sought to define cryptocurrencies since 2017 via Act No. 253/2008 Coll., on selected measures against legitimization of proceeds of crime and financing of terrorism.[70] The definition has been changed and broadened, effective

[64] Szabo, Septimiu, June 2020. 'Transition to Industry 4.0 in the Visegrad countries', European Commission,
[65] Ibid.
[66] Zahradnicek-Haas, Elizabeth, 'Meet the Czech company that's mainstreaming cryptocurrency around the world', Expats.cz, 29/4/2021. Accessed 21/9/2021.
[67] Interviewee 6.

[68] Globsec, 'Report 1 Visegrad Four: Countering the financing of terrorism while not directly threatened by terrorism', 25/5/2021. Accessed 4/8/2021.
[69] Ibid.
[70] Act No 253 / 2008 Sb. of 5 June 2008 on Selected Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism, See Section 4 of the Act.

since January 2021. [71] According to the methodological instruction of The Czech FIU, any crypto transaction with the equivalent of 15.000 EUR or higher should be reported and regarded as suspicious. However, this instruction has been hard to be implemented and thus became inapplicable because it causes a huge overload of information that needs to be analyzed with a little added value to actually detecting illicit funds or activities.

Conclusion

Cryptocurrencies make terrorists' financial activities harder to detect and prevent, although such actors generally raise, move, and spend money in remarkably ordinary ways. [72] The current terrorist threat to Europe refers to low-cost attacks, therefore, does not involve large sums of money or suspicious international transfers. The data presented in this paper shows that extremists in Europe are increasing their interest in using cryptocurrencies to spread propaganda and sustain their networks.

While the global use of cryptocurrencies is increasing, the EU has the challenge to regulate a technology, which is still evolving.

Cryptocurrencies are not entirely untraceable, but the national FIUs or a newly established EU financial intelligence agency should invest more resources in building the tools, expertise, and skills to trace when this is necessary. The law enforcement agencies in Central Europe should develop the tools and understanding of how to identify suspicious crypto transactions and deal with questions such as: who controls blockchain networks; how to extract knowledge about senders and receivers, and what the limitations are when innovations such as mixers and tumblers are involved. Countering terrorist financing, which involves cryptocurrencies, already requires enhanced technical capabilities at the national level along with faster exchange of relevant information between national FIUs in the EU. Considering the technological challenges that cryptocurrencies present, FIUs in the

[71] Act No. 253/2008 Coll. Act on Certain Measures against the Legalization of Proceeds from Crime and Terrorist Financing.

[72] Oftedal Emilie. 2015.

October 2021

Visegrad countries should adopt new instruments such as blockchain analysis and enhance their expertise in public and private key cryptography. As countries of the region do not have the capacity to conduct in-depth blockchain analyses individually, this can be done through either public-private partnerships, regional cooperation or to rely on a centralized EU agency.

About the author

Asya Metodieva, Ph.D. is a researcher at the Institute of International Relations Prague. Asya earned her Ph.D degree from Central European University Budapest/Vienna. Her research focuses on terrorism, mobilisation into radical movements, polarisation and information warfare. She wrote her Ph.D. on foreign fighters from the Western Balkans who joined the Syrian War. In addition to her academic work, Asya has published policy papers and analytical pieces with regional and international think thanks and media platforms such as Europeum, Stratpol, Visegrad Insight, Riddle, and Euronews.

This policy paper was produced within the Think Visegrad in Brussels Fellowship programme.

In the first half of 2016, eight think-tanks from the Visegrad Group that have been cooperating in the Think Visegrad platform, agreed on the idea proposed by the EUROPEUM Institute for European Policy, to create a common representation office in Brussels. The main motivation for it is the need to encourage debate on issues of common interest to the EU and the V4 and explain the positions of the V4 to a wide audience. Think Visegrad in Brussels would like to project an image of constructive partners, to explain the dynamics of the debates within our regions and to highlight our active contributions to EU policy-making.

For more information about Think Visegrad and its members visit www.thinkvisegrad.org.