Tanja MILOSHEVSKA

UDK:323.281:[336.746:004.91.056.55
Review article

DIGITAL CRYPTOCURRENCIES-NEW CONTEXT FOR TRANSNATIONAL TERRORIST ACTIVITIES

Abstract

Virtual currencies including cryptocurrencies such as Bitcoin have gotten significant popularity over the past several years. The paper's purpose is to comprehend whether terrorist organizations and terrorist groups are presently using cryptocurrencies to funding their activities and, if not, why they do not exploit such currencies. Cryptocurrencies are easy to use, secure, and if used correctly can hide identity. That would explain why increasing research reports claim that terrorists are using them to fund their actions. Is that claim true, and if so, to what extent? And are there any real-world examples to draw on? In particular, factors that tend to discourage use contain continued unpredictability in the cryptocurrency community, cooperation between international law enforcement and the intelligence community, and developments in regulation and enforcement. The question of whether terrorist organizations will use these systems is dependent on the available technology, as well as on these groups' needs and abilities.

Key words: *DIGITAL CRYPTOCURRENCIES, TRANSNATIONAL TERRORIST ACTIVITIES, DARK WEB, TERRORIST FUNDING.*

Introduction

There is a great need to understand the full potential for terrorist use of cryptocurrencies, including options for identifying and tracking their use, the sophistication and technological capability of terrorist groups, and the potential for such use to increase in the future, given expected technological developments (Dion-Schwarz at all., 2019).

However, the challenge posed by cryptocurrencies extends beyond Bitcoin. Many new cryptocurrencies have emerged in the past few years, including such alternative currencies (altcoins) as Omni Layer (MasterCoin), BlackCoin, and Monero, which are touted as more private and secure than Bitcoin. Zcash is another cryptocurrency that offers a higher degree of privacy and provides the potential ability to use and transfer currency offline, which could make it difficult for law enforcement to trace illicit transactions. Other cryptocurrencies, including Hawk, would allow fully private contracts and transactions on the Ethereum blockchain. Like Bitcoin, the Ethereum blockchain is a distributed computing platform and operating system (Dion-Schwarz at all., 2019).

Terminology

Cryptocurrency means a digital currency produced by a public network, rather than any government, that uses cryptography to make sure payments are sent and received safely (Cambridge Dictionary).

Digital refers to using an electronic system that uses a binary number to record sound or store information, and that gives high-quality results (Oxford Learner Dictionary, 2008).

Terrorism is the use of violence for political purposes. Terrorism is "the use of violence against random civilian targets in order to intimidate or to create generalized pervasive fear for the purpose of achieving political goals" (Yonah, 1976). The definition of terrorism has evolved over time, but its political, religious, and ideological goals have practically never changed (Sloan, 2006).

Today, terrorism has changed in terms of its dimension, actors, platform, and activities. Terrorism is an act of cyber hackings, drug trafficking, kidnappings, torture, assassinations, propaganda, sabotage, vandalism, aerial bombings, hijackings, suicide attacks that involved an act of violence toward society (Jackson at all, 2011).

This paper uses the organizational theory of terrorism initiated by Martha Crenshaw (2008). The organizational theory mostly discusses the objectives, actions, and internal dynamics of the terrorist organization. This theory emphasizes the main goal of a terrorist organization which is the survival that could be illustrated as the state institution or commercial enterprise. In responding to the external pressures, the terrorist organization will change its incentives through innovation (Ozdamar, 2008).

Potential for cryptocurrencies to facilitate terrorist finance operations

Terrorists require significant funding to carry out attacks and other activities. Indeed, there is reason to believe that, if terrorist groups were better funded overall, there might be more frequent, more successful, and larger attacks (Acharya, 2009). There are several reasons that support this belief.

First, more funds for operations would presumably lead to increased funding for the structures that enable these attacks, which include recruiting and training attackers and inspiring potential lone wolves.

Second, groups facing less monetary pressure (i.e., those that are better funded) also might be more willing to take risks, such as larger or riskier attacks (Shapiro, 2012).

Lastly, and perhaps more contentiously, increased funds can be used directly for additional and larger attacks. It might be difficult to directly link increased funds to terrorist attacks, although in specific documented cases, "the literature often describes shortages of cash as a problem for terrorist operations" (Oftedal, 2015).

Whether and how terrorist organizations would use a cryptocurrency system depends on the available technology and its properties, as well as on the organization's needs and capabilities. Newer cryptocurrencies might emerge with properties that terrorist organizations find more attractive than those of currently available cryptocurrencies. For instance, if a future cryptocurrency provides better anonymity than Bitcoin for large-sum transactions and is more widely adopted than Zcash, then terrorist organizations might be willing to employ that currency for specific activities. Thus, it is important to look at individual terrorist groups to analyze what they would need from cryptocurrencies and compare those needs with the properties of available cryptocurrencies.

Bitcoin is continuously utilized by the purchasers and consumers of illicit goods on the Dark Web. A report titled "Terrorist Use of Virtual Currencies: Containing the Potential Threat" stated that terrorist organizations have used cryptocurrencies to support the survival of their organizations. For instance, the terrorist organization in the Gaza Strip have used cryptocurrencies to fund their operations as well as the Islamic State in Iraq and Syria (ISIS) members and supporters who particularly used the cryptocurrencies recorded in Indonesia and United States. Noting further that the substantial and abrupt loss of their physical territory, as well as the proliferation of strict military operations, may limit their access and make them more difficult to move their cash across geographic areas and borders or the traditional financial transaction called *hawala* which refers to the physical financial transaction by using a local broker to transfer money between locations (Ward, 2018). Thus, this phenomenon potentially encourages terrorist organizations to explore the new technology that could support their ability to move funds through cryptocurrencies.

In the paper, we considered a set of examples: specifically, al Qaeda and affiliates, the Islamic State of Iraq and Syria (ISIS), Hezbollah, narcoterrorist organizations, and lone-wolf attackers. Although these groups differ in their goals, their need for anonymous, secure, and ready streams of funding make cryptocurrencies of some potential value to them. For these groups, we examined five financial activities (fundraising, illegal drug, and arms trafficking, remittance and transfer of funds, attack funding, and operational funding) and evaluated the importance of cryptocurrency properties in facilitating these activities (Dion-Schwarz et al., 2019).

There are various ways in which virtual cryptocurrencies may be used by terrorist groups. Organizations may use the Dark Web for obtaining weapons, including traditional firearms, explosives, chemical or biological toxins, paying for these with virtual cryptocurrencies. Virtual cryptocurrencies could also facilitate other illicit income activities by terrorist groups; there has been for instance a virtual cryptocurrency demands during kidnapping for ransom, with kidnaping for ransom being a popular source of income also for terrorist organizations. Similarly, if terrorist organizations move toward more digital attacks or cyberterrorism, virtual cryptocurrencies may become more useful to these organizations as they allow for the purchase of "digital weapons" such

as malware. Obviously, virtual cryptocurrencies are not crucial to any of these activities, but they could make these transactions easier than traditional card payments or bank transfers (Entermann and Berg, 2018).

An additional aspect that may speed up terrorist groups' adoption of virtual cryptocurrencies is the convergence of terrorist and criminal organizations. Terrorist groups have long used organized criminal means, such as tobacco smuggling, to fund their activities and there are numerous examples of cooperation between the two types of groups. These range from ETA's relationship with Columbian drug cartels and facilitation of cocaine smuggling in Europe, to the Continuity IRA's cooperation with Eastern European human traffickers and Hezbollah's cooperation with Mexican drug lords. More recently, there has been an increased emphasis on the so-called crime-terror nexus, for example through the movement of individuals with criminal pasts into terrorist networks. At least two-thirds of individuals with an operational connection to IS who carried out attacks in Europe and America in the past few years had a criminal past (Basra, Neumann, 2017). There is evidence that the criminal "skills" such as access to forged documents and weapons are readily used in their new extremist environments. Given these developments, it may just be a matter of time until the virtual cryptocurrencies tools and tactics used by criminal syndicates are exported to terrorist groups; or that cooperation and transactions between terrorist and organized criminals could involve virtual cryptocurrencies (Entermann and Berg, 2018).

These properties are anonymity, usability, security, acceptance, reliability, and volume. By *anonymity*, we mean the ability to hide and protect the identity of the user. *Usability* refers to the ease with which the user can conduct transactions and manage his or her own currency.

Security refers to the degree to which the cryptocurrency infrastructure secures the confidentiality, integrity, and accuracy of transactions and user accounts. By *acceptance*, we mean the degree to which the currency is accepted by a user community as well as the size of the community of users. *Reliability* refers to the speed and availability of transactions, as viewed by users. Finally, *volume* refers to the time-averaged aggregate size of transactions in the cryptocurrency infrastructure.

Terrorist organizations' current and future needs for cryptocurrency

The question of whether and how terrorist organizations would use a cryptocurrency system depends on the available technology and its properties, as well as the groups' needs and capabilities. Newer cryptocurrencies may emerge with properties that terrorist organizations find more attractive than those of currently available cryptocurrencies. For instance, if a future cryptocurrency provides better anonymity than Bitcoin for large-sum transactions and is more widely adopted than Zcash, then terrorist organizations might be willing to employ that currency for specific activities. Thus, it is important to look at in-

dividual terrorist groups to analyze what they would need from cryptocurrencies and compare those needs with the properties of available cryptocurrencies (Dion-Schwarz et al., 2019).

However, particularly with improved usability, cryptocurrencies such as Bitcoin may be appealing to use in fundraising, and some evidence is emerging that terrorist organizations may be using cryptocurrencies for this purpose (Stalinsky, 2018).

Modern cryptocurrencies are potentially much more flexible, and this may create challenges in financial accounting that look like those involved in attributing and preventing computer intrusions. The field of cryptocurrencies is much less certain, much more dynamic, and one in which innovations might allow terrorist groups to circumvent monitoring. On the other hand, it is a field where sophistication matters; money laundering may be made harder to detect when conducted by sophisticated actors, but many terrorist groups' technical abilities are not currently suited to this type of activity (Dion-Schwarz et al., 2019).

Increased use of cryptocurrencies in complementary and adjacent markets could indicate their increased viability among terrorist organizations. Some counterfeiting operations have begun to use darknet markets, and there is a significant trade in stolen credit cards and identities in these markets (Aliens, 2012).

Broad Role	Specific Cases	Description
Dark Web as an enabler of anonymous Financial Transactions	Using Bitcoin over Tor for anonymity	An added layer of anonymity and precaution (DiPiero, 2017).
	Money Laundering of cryptocurrencies via tumbling services	Specific services to launder money, e.g. via bitcoin conversion (Dalins et al., 2017).

There are several illicit purposes of the utilization of cryptocurrencies by terrorist organizations such as purchasing drugs, selling drugs, weapons, and afford illicit services on the Dark Web. Moreover, the terrorist organization also launched its donation through cryptocurrencies. It could be inferred that cryptocurrencies could be turned into ransom payments. In addition, there are several cryptocurrencies features that provide advantages for the users such as being better than cash or credit, exchangeable for goods and services, convertibility, and stability of value (balance price volatility) (Everette, 2017).

Documented examples of terrorist acquisition of cryptocurrency

Terrorist networks have adapted to technology, conducting complex financial transactions in the digital world, including through cryptocurrencies (The US Department of Justice, 2020).

Based on the study conducted by RAND Europe titled "Behind The Curtain: The Illicit Trade of Firearms, Explosives, and Ammunition on The Dark Web," there is a direct link between Paris and Munich terrorist attack as well as the arms dealing within the Dark Web through cryptocurrencies. The study shows that there were 24 French and British cryptocurrencies markets on the Dark Web along September 2016 where 75 percent of the transactions proved to conduct arms dealing (Everette, 2017). The weapons used by the attackers and could be related to the ISIS propaganda which called for the proliferation of simplistic attacks by using vehicles, firearms, weaponry, chemical weapons, and knives. Moreover, the al-Qaeda linked organization namely *al-Sadaqah* accused of using Facebook and Telegram to launch their financial campaign through Bitcoin (Malik, 2018).

Over the past year, terrorist groups have pivoted to acquiring and storing wealth in virtual currencies like Bitcoin. In August 2020, the US Department of Justice (DOJ) announced the largest seizure to date of crypto-assets associated with terrorist groups. The DOJ announced that it had seized the equivalent of millions of dollars across more than 300 cryptocurrency accounts associated with three U.S. designated Foreign Terrorist Organizations (FTOs), namely Hamas, Al-Qaeda, and the so-called Islamic State. In 2019, Hamas's military wing started an online cryptocurrency fundraising campaign using social media tools to encourage anonymous donations. Contrary to popular belief, the anonymity often associated with cryptocurrencies is a misnomer. The Hamas scheme consequently unraveled, with 150 cryptocurrency accounts seized. Al-Qaeda has also branched out into using social media tools to generate donor interest with the objective of supporting its activities in Syria through cryptocurrency. In the case of al-Qaeda, the DOJ seized more than 100 cryptocurrency accounts. Both Hamas and al-Qaeda's interest in cryptocurrency, respectively, predated the DOJ announcement, but this funding stream has garnered far less attention relative to other sources of financing (IntrelBrief, 2020).

Like Hamas and al-Qaeda, ISIS was implicated in the Department of Justice's August 2020 announcement. And, similar to both Hamas and al-Qaeda, ISIS-linked individuals being involved in crypto-currency schemes is not novel. In 2017, Zoobia Shahnaz provided $85,000 to ISIS by maxing out credit cards to purchase Bitcoin and then later converting the Bitcoin to cash to obfuscate her activities. Two years prior to Shahnaz's scheme, Ali Shukri Amin pleaded guilty to providing material support to ISIS by showing people how to acquire and send Bitcoin to the group. The more recent cryptocurrency effort was conducted by Murat Cakar, an ISIS hacker (and connected to Shahnaz) who created a website purporting to sell personal protective equipment (PPE), including N95

facemasks, for profit. Given the COVID-19 outbreak and the difficulties associated with in-person financing ventures, the August 2020 cases could represent a pivot by organized terrorist groups toward the acquisition of virtual assets. ISIS in particular is likely to continue efforts to accumulate wealth through cyber-enabled operations, some of which could involve cryptocurrency (Soufan Center, 2020).

At the beginning of 2019, the al-Qassam Brigades posted a call on its social media page for bitcoin donations to fund its campaign of terror. The al-Qassam Brigades then moved this request to its official websites, alqassam.net, alqassam.ps, and qassam.ps. However, such donations were not anonymous. Working together, IRS, HSI, and FBI agents tracked and seized all 150 cryptocurrency accounts that laundered funds to and from the al-Qassam Brigades' accounts.

In 2020, the Financial Action Task Force (FATF), an inter-governmental body, highlighted the possible uptick in terrorist interest in cryptocurrency, especially during the COVID-19 pandemic. In May, FATF released a report arguing that the coronavirus pandemic could lead to an 'increase misuse of online financial services and virtual assets to move and conceal illicit funds'. Less than one month after the DOJ announcement, FATF published another report on red flag indicators, noting that virtual assets could be used by terrorist financiers and money launderers. The indicators range from unique transaction patterns to geographic risk profiles that could indicate the misuse of virtual assets. For Financial Intelligence Units, virtual asset service providers, and financial institutions, these indicators provide useful guidelines for countering the use of cryptocurrency by a range of illicit actors. Despite the FATF guidelines and the August 2020 move by the United States to seize and seek the forfeiture of Hamas, al-Qaeda, and ISIS financial assets, terrorists are increasingly likely to use cryptocurrency to accumulate and store wealth. This path is especially probable due to the likely continued reliance on 'virtual' conduct of business even after COVID-19 vaccines are distributed throughout 2021. As more everyday consumers use cryptocurrencies, the opportunities for terrorists will increase, as they seek cover and concealment amidst the increased volume of overall transactions (Soufan Center, 2020).

Terrorists use virtual currencies to evade detection and to fundraise: terrorists, like criminals, use cryptocurrency because it provides the same form of anonymity in the financial setting as encryption does for communication systems (Weimann, 2016).

Overall, the use of cryptocurrencies should be seen as part of a general shift towards online terrorism (Casadei Bernardi, 2019).

This paper shows that should a cryptocurrency appear that provides extensive implementation, better anonymity, enhanced security, and that is subject to unreliable regulation, then the possible utility of this cryptocurrency, as well as the potential for its use by terrorist organizations, would grow.

Conclusion

Concerns about the usage of cryptocurrency to allow terrorist activities have yet to be evident, but coming developments in cryptocurrency technologies will likely have a significant long-term consequence on terrorism finance. The speed at which these technologies are accepted, and the details of which technologies are used and how they are organized, are critical uncertainties that have important operational impacts. This paper proposes that regulation of cryptocurrencies, along with international collaboration among law enforcement and the intelligence, would be imperative steps to prevent terrorist organizations from using cryptocurrencies to funding their activities.

Security in the cryptocurrency environment is of moderate to high position for terrorist organizations because existing cryptocurrencies are exposed to a diversity of cyberattacks.

Still, newfangled currencies that are thought to advance security are issue to significant scrutiny as new security vulnerabilities are discovered over time. When we analyze all our assessments together, including such other significant factors as the consistency and capacity of the cryptocurrency market, we find that no existing cryptocurrency can address all of the terrorist organizations' financial needs.

References:

Acharya, A. (2009). *Targeting Terrorist Financing: International Cooperation and New Regimes*, New York: Routledge.

Aliens, C (2016). "Darknet Bust: Global Law Enforcement Raids Massive Counterfeiting Organization," *Deep.Dot.Web*, December 17.

Basra R., Neumann P.R. (2017). Development in the crime-terror nexus in Europe, *CTCSentinel*, Vol.10, Issue 9, Combating Terrorism Centre at West Point, USA.

Cambridge Dictionary, "Cryptocurrency," *Cambridge Dictionary.* Available at: https://dictionary.cambridge.org/dictionary/english/cryptocurrency

Casadei B. (2019). Terrorist Use of Cryptocurrencies-A Blockchain Compliance White Paper, Blockchain Consultus, London, United Kingdom.

Crenshaw, M. (2008). Theories of terrorism: Instrumental and organizational approaches, *Journal of Strategic Studies*, Volume 10.

Dalins, J. at al. (2017). *Criminal motivation on the dark web: A categorisation model for law enforcement.* Digit. Investig.

DiPiero, C. (2017). Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web. U. *Ill. L. Rev*.1267.

Enternmann, E., Willem van der Berg. (2018). *Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?* International Centre for Countering Terrorism, Hague.

Everette J, (2017) *Public-Private Analytic Exchange Program: Risks and Vulnerabilities of Virtual Currency,* Washington: Director of National Intelligence.

IntelBrief (2020). IntelBrief: Terrorists' Use of Cryptocurrency, The Soufan Center, New York, USA, December 10. Available at: https://thesoufancenter.org/intelbrief-2020-december-10/ [Accessed 12 February 2021].

Jackson, R at all. (2011). *Terrorism: A Critical Introduction,* Palgrave Macmillan.

Malik, N. (2018). "How Criminals And Terrorists Use Cryptocurrency: And How To Stop It," *Forbes,* August 31st. Available at: https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and terrorists-use-cryptocurrency-and-how-to-stop-it/#6766399a3990. [Accessed 16 April 2021].

Oftedal, E. (2015). *The Financing of Jihadi Terrorist Cells in Europe*, Norway: Forsvarets Forskningsinstitutt.

Oxford Learner Dictionary. (2008). *Fourth Edition,* China: Oxford University Press.

Ozdamar, O. (2008). "Theorizing Terrorist Behavior: Major Approaches and Their Characteristics", *Defence Against Terrorism Review 1,* No. 2.

Shapiro, J. N. (2012) "Terrorist Decision-Making: Insights from Economics and Political Science," *Perspectives on Terrorism*, Vol. 6, No. 4–5.

Sloan, S. (2006). *Terrorism: The Present Threat in Context*. Oxford: Berg Publishers.

Stalinsky, S. (2018). "The Cryptocurrency-Terrorism Connection Is Too Big to Ignore," *Washington Post*, December 17.

The United States Department of Justice (2020). Office of Public Affairs, *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*, August 13. Available at: https://www.justice.gov/opa/pr/global-disruption-three-terror- finance-cyber-enabled-campaigns. [Accessed 12 February 2021].

Ward, A. (2018). "Bitcoin and the Dark Web: The New Terrorist Threat?" *RAND Corporation,* January. Available at: https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html [Accessed 15 March 2021].

Weimann, G. (2016). "Going Dark: Terrorism on the Dark Web", *Studies in Conflict & Terrorism* 39, 195-206. Available at: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546. [Accessed 12 February 2020].

Yonah, A. (1976). *International Terrorism: National, Regional and Global Perspectives.* New York: Praeger.