ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

10
2019

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

10

ISSUE 2/2019

Milano 2019

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE 2 – 10/2019

Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442
ISSN DIGITALE: 2533-0659
ISBN: 978-88-9335-540-7

copertina: progetto grafico Studio Editoriale EDUCatt

Table of contents

The decentralized finance-violent extremism nexus: ideologies, technical skills, strong and weak points

Daniele Barone

Nota autore

Daniele Barone is a researcher and an analyst in the security sector. Graduated in Marketing & Communication at IULM University, he has a master's degree in International Relations at ASERI Graduate School of Economics and International Relations – Catholic University of the Sacred Heart. He specialized in homeland security and counter-terrorism studies earning an Executive Certificate in Counter-Terrorism studies at the International Institute for Counter-Terrorism (ICT) – Herzliya.
He has worked, for more than five years, as a project manager and a digital marketing specialist in the private sector.
Given his experience in online communication, economics, and geopolitics, his research interests are related to cyber-jihad, terrorism financing, and terrorist groups' communication strategies.

Abstract

Il comune denominatore dell'utilizzo delle criptovalute da parte dei gruppi terroristici ha origine dall'inquadramento legale poco chiaro in cui le criptovalute attualmente operano. Tale contesto permette, seppur indirettamente, la proliferazione di una propaganda basta sul rifiuto dell'idea di Stato, descrivendo la gestione decentralizzata delle criptovalute come un mezzo di pagamento che appartiene esclusivamente al popolo e supera le interferenze prodotte dal controllo centralizzato del governo o di altri intermediari.
Concentrando l'analisi sulla giustificazione ideologica e gli opachi schemi di finanziamento messi in atto da organizzazioni terroristiche internazionali come Hamas, movimenti globali come i gruppi estremisti di estrema destra ed i loro simpatizzanti, poi descrivendo come piccoli gruppi mercenari jihadisti come il Malhama Tactical Team o campagne di donazione con scopi umanitari sospette stanno evolvendo le proprie competenze nei settori della comunicazione online e delle criptovalute, questa ricerca fornirà una visione sia generale che particolare degli attuali collegamenti terrorismo-FinTech. L'analisi spiegherà come, nonostante le competenze tecniche dei gruppi estremisti in questo settore sembrino essere ancora in fase embrionale, presentano imminenti prospettive di miglioramento, creando una diffusione a cascata di know-how e giustificazioni ideologiche e politiche. Queste caratteristiche del fenomeno possono generare un duplice risultato: trasformare il finanziamento al terrorismo in un'occasione senza precedenti per migliorare le tecniche investigative ed i metodi di analisi o, al contrario, rendere l'utilizzo per fini terroristici della finanza moderna un settore sempre più complesso da monitorare.

The common denominator in the exploitation of cryptocurrencies by terrorist groups, can be found in the grey legal framework where cryptocurrencies operate. This contest, even though indirectly, allows the diffusion of a propaganda related to the rejection of the idea of State, by depicting the decentralized control of cryptocurrencies as a mean of payment that belongs exclusively to the people, avoiding the interference of a centralized government control or any sort of middleman. Focusing on the analysis of the ideological justification and opaque financing patterns used by international organizations as Hamas, global movements as alt-right extremist groups and their sympathizers, then describing in depth how small jihadist private military contractors as the Malhama Tactical Team or suspicious online humanitarian crowdfunding campaigns are developing their skills both in the online communication and in the cryptocurrency field, this essay is aimed at providing an either overall or specific view of the current terrorism-FinTech nexus. It will explain how, even though extremist groups' skills in the cryptocurrency sector may seem at an infancy level, they are evolving very fast and creating a trickle-down diffusion of know-how and ideological or political justifications. These elements can generate a twofold outcome: turn terrorism financing into an unprecedented occasion to improve investigative and analysis methods or, on the other hand, turn exploitation of modern finance for terrorism purposes into a total undetectable sector.

Keywords

Jihad, Alt-right, Financing, Cryptocurrency, Cybercrime

Introduction

Between the end of 2018 and the first half of 2019, many extremist political or religious groups have exploited the anonymity of cryptocurrencies. In particular, small or structured international jihadist groups have been experimenting online financing methods to find alternative means to receive donations, while far-right extremist groups have been using them to store and invest money or organize international crowdfunding campaigns.

Besides these differences, the common denominator in terrorists exploitation of cryptocurrencies can be found in the grey legal framework where many areas of modern finance are currently operating, allowing the proliferation of factions promoting an extremist narrative related to the rejection of the idea of State, fuelled by displaying and encouraging the use of a mean of payment that belongs exclusively to the people, overlapping the interference of a centralized governmental control or middleman.

Furthermore, the need for extremist groups to spread their propaganda through the web is giving them more and more access to cutting-edge technical expertise. The two areas are linked by an ongoing innovation process of their ability aimed at evading detection, developing their technical capabilities and calling for donations in cryptocurrencies through legitimate services like social media or public websites, increasing the chances to freely interact with many actors involved in cybercrime or hacking at various levels.

Indeed, international extremist groups (both political and religious), activists, and sympathizers scattered across the globe are still adapting more and more to either the developments in the ICT sector as a physiological response to the territorial instability of their groups. From this lens, these violent organizations are not only taking advantage of online tools which are already mainstream as social media or end-to-end chats, but also evolving in using up-to-date and not yet widespread online products and services as cryptocurrencies, encryption keys, cybersecurity issues, and alternative web hosting services, which require a medium/high e-skills level. From this perspective, they are on the one hand transversally learning from their members or related groups (as, for instance, in the case of *Amaq News Agency* and alt-right groups, creating a ZeroNet account after *Cyber Caliphate* hacking group, *Ansar Al-Khilafah*, previously experimented it) on the other hand, teaching their audience how to use modern online tools to communicate, finance the organization, and access to violent contents in a climate of total anonymity through the web.

This paper will focus on the latest developments (2018/2019) of those either technical or ideological aspects which are likely to spread more and more the use of modern finance to raise money for violent extremist groups.

Focusing the analysis on the ideological justifications and financing patterns put into action by international organizations as Hamas or global movements as alt-right extremist groups, then describing in depth how small jihadist private military contractors as the Malhama Tactical Team or opaque online crowdfunding campaigns are developing their expertise both in the communication and in the cryptocurrency field, this essay is aimed at providing an either overall or specific view of the current terrorism-FinTech nexus. It will explain how, even though extremist groups' technical skills in the cryptocurrency sector may seem at an infancy level, they are still evolving fast and creating a trickle-down diffusion of skills and ideological justifications which may turn terrorism financing into a more and more undetectable sector.

1. Latest technical developments in the illegal exploitation of cryptocurrencies: Europol IOCTA 2018

The latest report of Europol on Internet Organized Cyber Crime (IOCTA 2018)[1] discusses, among other issues, the weak points that modern financial

[1] Europol (2018) I*nternet Organised Crime Threat Assessment (IOCTA) 2018*. European Union Agency for Law Enforcement Cooperation. Available at https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.

tools and a lack of either an up-to-date legal framework or cooperation among institutions and the private sector, brings to the cybercrime field.

The report highlights many sectors which are likely to become a target for criminal and terrorist purposes and depicts the latest development in the misuse of cryptocurrencies at different levels: Cybercrime in general (petty or organized crime) - Jihadist networks (local or international) - modern cyber-threats cryptocurrency related.

According to IOCTA 2018, even though Bitcoin has lost its majority of the overall cryptocurrency market share (Bitcoin enjoyed over 80% of the cryptocurrency market share, but by the start of 2017 this had dropped to less than 35%), it still remains the primary cryptocurrency encountered by law enforcement.

In particular, Bitcoin is still the most widely used cryptocurrency on **Darknet illegal markets**. According to Europol, even though law enforcement has taken down three major Darknet markets (i.e. AlphaBay, Hansa, and RAMP), it is reported a significant growth in both the number of small vendor shops (shops run by a single vendor) and secondary markets (i.e. non-English language markets) dedicated to a particular nationality or language group.

Nevertheless, nowadays Bitcoin is not anymore able to provide as much anonymity as it did in the past. As demonstrated by Philip and Diana Koshy in 2014, which were able to identify the IP addresses connected to more than 1000 Bitcoin addresses[2], it is possible to find a breach in the wall of the partially anonymous Bitcoin transactions flow.[3] Moreover, law enforcement has already proved to be able to track down and reveal Bitcoin **mixing services** (i.e. protect the anonymity of transactions by mixing many users' Bitcoin reserves with each other) used by criminals to launder money.

Furthermore, Bitcoin is developed with the Blockchain technology where data flow between computers (called "nodes") like gossip in a crowd, becoming immutable and unchangeably bound with each other. In this term, even though Blockchain is structured in order to protect users' real identity behind encryption codes, it also allows making public information (and public record) of their entire financial history[4]. Hence, from an investigative and monitoring perspective, get only once a criminal committing a crime by using Bitcoins, allows to uncover his whole criminal history.

[2] P. Koshy D. Koshy P. McDaniel (2014) *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*. Pennsylvania State University, University Park, PA 16802, USA. Available at https://pdfs.semanticscholar.org/c277/62257f068fdbb2ad34e8f787d8af13fac7d1.pdf.

[3] J. Bohannon (March 9, 2016) Why criminals can't hide behind Bitcoin. ScienceMag. Available at http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

[4] K. Marinos (March 23, 2016) *Are Bitcoin Transactions Traceable?*. CoinTelegraph. Available at https://cointelegraph.com/news/are-bitcoin-transactions-traceable.

This is likely to cause a significant shift of cybercriminals to more privacy-centric types of cryptocurrencies in the very near future[5].

1.1 Every internet user is unwittingly becoming a victim: Cryptojacking, a hallmark for modern cybercrime

Cryptojacking is the unauthorized use of a computer, tablet, mobile phone, or connected home devices by cybercriminals to mine for cryptocurrency.

There are only a finite number of Bitcoins that have not been completely mined and they can be mined only by solving a complex and ever-growing math task "**proof of work",** which requires elevated electricity bills and expensive computer equipment. Thus, the more devices are working, the faster is possible to mine coins, and cryptojacking allows cybercriminals to use other people's devices to pursue this task. Cryptojacking can occur in two ways:

- **Phishing tactics**, running a code that downloads the cryptomining script on the victims' computer, the most common method is to send the malware by email.
- **In-browser miner**, injecting a cryptomining script on a website or on an online advertisement that is placed on multiple websites. The script runs on the visited website, so the code does not need to be installed or the user doesn't even have to opt-in[6].

In both cases, the code solves complex mathematical problems and sends the results to the hacker's server while the victim is completely unaware.[7]

In-browser based cryptojacking **is not illegal**, thus it is more appealing to cybercriminals wishing to keep a low profile, requiring little or no victim engagement and, at least currently, minimal law enforcement attention.

Hence, for all these reasons, cryptojacking is expected to become a regular, low-risk revenue resource for cybercriminals.

1.2 Cyber-attacks targeting users and facilitators

Quoting Europol IOCTA 2018 "in a trend mirroring attacks on banks and their customers, cryptocurrency users and facilitators have become victims of cybercrimes themselves... Money launderers have evolved to use cryptocur-

[5] O. Kharif (January 2, 2018) *The Criminal Underworld Is Dropping Bitcoin for Another Currency*. Bloomberg. Available at https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency.

[6] https://hackerbits.com/programming/what-is-cryptojacking.

[7] https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html.

rencies in their operations and are increasingly facilitated by new developments such as decentralized exchanges which allow exchanges without any Know Your Customer requirements".

Indeed, a consequence of the decentralized and unregulated system of cryptocurrencies and the fact that they are becoming more mainstream (almost **1600 listed cryptocurrencies**), is that cryptocurrency users, exchange platforms and mining services are now subjected to the same attacks aimed at traditional financial instruments.

The most commons kinds of cyber-attacks and targets are the following:

- Phishing tactics aimed at taking over users' **login credentials for their online exchanger accounts, electronic wallets, and private keys.**
- **Exchange services**, which hold their own number of cryptocurrencies for trading and the fund of their customers who purchased cryptocurrencies, are key targets for cybercriminals given the huge amount of money that they administrate ore store for their customers. As the hacking attack to the Italian exchanger **BitGrail** that resulted in the correspondent loss of USD 195.000.000.
- Attack to cryptocurrency exchange services to **steal customers' data to further fraud** as, for instance, "phishing customers for their account login credentials and subsequent currency theft".

1.3 Jihadist networks experiment

The Europol 2018 report defines Islamic terrorists' cyber attack expertise as at its infancy level. It describes Islamic terrorist groups as very high-skilled in terms of online propaganda through the masterly use of social media, surface or deep web forums or blogs, and end-to-end encrypted chat services, but still without an elevated overall harmful cybercrime potential. Nevertheless, IOCTA 2018 shows some interesting trends, about terrorist groups' cutting-edge technical expertise in the use of cryptocurrencies, which are worth explaining.

- **A few actors with high-degree technical know-how**: as already analysed by ITSTIME[8], since 2012 there have been a few cases related to terrorist groups' use of cryptocurrencies, mostly under the form of either more or less explicit online crowdfunding campaigns. The Europol report rightly defines this initial phase as the "Jihadist networks experiment with cryptocurrencies". During this experimental stage, a

[8] http://www.itstime.it/w/bitcoin-and-other-types-of-cryptocurrency-modern-and-undetectable-ways-to-finance-terrorism-by-daniele-maria-barone.

common denominator can be identified in the difficulty to track terrorists' transaction movements.

– **Privacy-centric cryptocurrencies**: as previously explained, Bitcoin is not the most anonymous choice in the cryptocurrency landscape. There already exist other types of cryptocurrency created with the primary purpose of protecting users' privacy. The most popular are Monero (launched in 2013) and Zcash (launched in 2016). Monero and Zcash respectively use *CryptoNote protocol*, which allows seeing only an approximate amount of money that was sent in the transaction,[9] and *Zk-Snark*, "Zero-knowledge", which allows one party to prove to another that a statement is true, without revealing any other information beyond the validity of the statement itself[10]. The competition among these privacy-centric cryptocurrencies is causing a fast-paced development entirely aimed at increasing their users' privacy[11] while becoming more and more user-friendly and widespread[12]. As in the *Akhbar alMuslimin case*, Islamic Terrorist groups have already proved to have a high degree of sophistication in exploiting modern methods to obscure their illicit funding. In fact, Europol has noticed that Daesh requested donations in Zcash and also used such cryptocurrency to purchase website domains. Even though Europol underlines that there is no proof of Zcash, or any other type of cryptocurrency, being used to finance any attacks on European soil, the development in this field deserves to be carefully monitored.

The evolution in the field of online terrorism financing previously described, may be reassumed by the latest development regarding the pro-Daesh renewed deep web crowdfunding campaign, **Akhbar al-Muslimin (Muslim news)**, an IS-affiliated website which published news from the Islamic State. In November 2017, one month after the fall of Raqqa, a banner for donations of Bitcoins was launched on the website. In particular, it posted a link for Bitcoin donations claiming, "Click here to donate Bitcoins to the (*Akhbar al-Muslimin*) website – do not donate from *zakāt*[13] funds". The donations are presented as a support for the web-

[9] https://www.worldcryptoindex.com/what-is-cryptonote-technology.

[10] https://z.cash/technology/zksnarks.

[11] E. Spagnuolo (April 26, 2017) Addio Bitcoin, nel deep web ora si paga con Monero e Zcash. Wired - Italia. https://www.wired.it/economia/finanza/2017/04/26/bitcoin-monero-zcash.

[12] D. Manheim, P.B. Johnston, J. Baron, C. Dion-Schwarz (April 21, 2017) *Are Terrorists Using Cryptocurrencies?* RAND Corporation. Available at https://www.rand.org/blog/2017/04/are-terrorists-using-cryptocurrencies.html.

[13] An Arabic word referring to a payment made annually under Islamic law on certain kinds of property and used for charitable and religious purposes, one of the Five Pillars of Islam. The

site, but may probably have been used by Daesh to restore its propaganda machine or fund terrorist attacks abroad[14]. The bitcoin address had no time to receive any donation because of two reasons: it was shut down after a while by authorities. Thus, it had no protection against Distributed Denial of Service attacks (DDoS) and only a bitcoin address to send donations, with no instructions or explanations available for users who were willing to donate to the website.

After the more consistent defeat of Daesh in Syria, on January 2019[15], the website reappeared online with a new bitcoin address. What is new is that, once the site has been accessed, now almost every page contains a request for a donation for "the activities of the website" that leads to the address of a virtual wallet for depositing the funds[16].

Furthermore, there are some new features added by the creators of the renewed website that give some interesting clues about an improved knowledge on how to facilitate the donation process:

- Because of the frequent closing of the *Akhbar al-Muslimin* website, the first window contains instructions for **finding the site's most updated links**: by sending an empty email to the address given, the user is automatically answered with an updated link to a mirror site of *Akhbar al-Muslimin*.
- There are more instructions available about how to exchange money into bitcoin with a link to explanatory videos about how cryptocurrencies work and to the designated exchange service platforms. On the first renewed version (January 2019) the exchange service used was VirWoX, a virtual currency trading company that allows buying **bitcoin via PayPal**[17]. Since March 9, 2019, the site referred potential donors to LocalBitcoins[18], a virtual currency money trading company where, to buy bitcoins, **providing identification is voluntary**.

word *zakāt* origins comes from Persian and Kurdu languages, meaning "almsgiving".

[14] D.M. Barone (2018) *Jihadists' use of cryptocurrencies: undetectable ways to finance terrorism*. Sicurezza Terrorismo e Società. http://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2018/11/Daniele-Maria-Barone-Jihadists%E2%80%99-use-of-cryptocurrencies_undetectable-ways-to-finance-terrorism.pdf.

[15] (February 12, 2019) *Drive for donations using Bitcoin on an ISIS affiliated website*. The Meir Amit Intelligence and Terrorism Information Center. https://www.terrorism-info.org.il/app/uploads/2019/02/E_018_19.pdf.

[16] (March 7, 2019) *Funding Terrorism: ISIS raises funds through an affiliated website, using bitcoins*. The Meir Amit Intelligence and Terrorism Information Center. https://www.terrorism-info.org.il/app/uploads/2019/03/E_054_19.pdf.

[17] https://www.virwox.com/help.php.

[18] https://localbitcoins.com/faq.

1.4 Suggested Improvements

This year's happenings in the online extremist groups financing field are providing new strong and weak points related to the illegal use of cryptocurrencies along with scope for improvement.

- **Improve Public Awareness**: Cryptocurrencies are becoming widespread, user-friendly and, in many cases, developing through a privacy-centric protocol, while institutions have not yet enough tools to properly investigate or prevent their illegal use. Help investors to avoid becoming unknowing victims of criminal or terrorist networks is fundamental. Institutions should put more efforts in giving clear instructions to these modern customers aimed at avoiding credential or private keys theft and guide them through a conscious way to invest in cryptocurrencies.
- **Introduce mandatory KYC procedures:** even though in many cases governments can't impose strict rules on cryptocurrency development companies or cooperate with them, it is still possible to cooperate with exchange services. Obligatory Know Your Customer procedures for exchange services or crypto debit/credit cards providers, would definitely help to prevent jihadists' donation campaigns or criminal frauds.
- **An updated legal framework:** many frauds or theft committed in the cryptocurrency field can't even be prosecuted. A flexible legal framework updated to modern financial threats is crucial to isolate the dangers in this field and let either investors or prosecutors' freedom of movement inside a clearly legal environment. Furthermore, this would be a strong deterrence for many individuals planning to commit financial cybercrimes.

2. Structured and International jihadist groups: Hamas crowdfunding bitcoin

On January 29, 2019, Abu Obeida, the spokesman for *Izz ad-Din al-Qassam*, the armed wing of the Hamas, announced that the group is now accepting donations in bitcoin[19]. An attempt to get around international restrictions on funding the organization, by circumventing the banking system and international anti-money laundering (AML) measures.

Originating in 1987 after the beginning of the first Intifada as a spinoff of Egypt's Muslim Brotherhood, and funded on the long-term goal of establish-

[19] M. Arnold, S.A. Ramadan (January 30, 2018) *Hamas Calls on Supporters to Donate to Group in Bitcoin*. Bloomberg. https://www.bloomberg.com/news/articles/2019-01-30/hamas-calls-on-supporters-to-donate-to-group-in-bitcoin.

ing strong Islamic states on all Palestinian territories by declaring war to Israel[20], Hamas (*Ḥarakat al-Muqāwamah al-'Islāmiyyah*)[21] is the Islamist group that for eleven years has ruled the Gaza Strip.

Perceptions of the group differ: Israel, US[22], Canada, EU, Japan, Egypt, among others[23], say it's a terrorist group that poses a grave obstacle to peace between Israelis and Palestinians, others argue it is a true representative of Palestinians[24] that won credibility with its grassroots charitable work and for being less corrupt than its rival, the Fatah faction of Palestinian Authority, which was Israel's partner in peace talks[25].

2.1 The group's Economic Resources

Hamas raises money prevalently from taxes (e.g. cigarettes, auto registration fees, goods coming from Israel[26]) and also regulates many types of businesses (e.g. street vendors, money-changing companies) requiring them to pay license fees. Hamas has also control over various Gaza resources, such as leasing government-owned heavy machinery to private contractors for a daily fee (one of many ways the group has been able to indirectly benefit from the international reconstruction funds flowing into Gaza).

Nevertheless, most of the group's economic resources come from donations either from activists/sympathizers[27] or from some Arab States sponsor-

[20] M. Levitt, D. Ross (2007) *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*. Yale University Press.

[21] Hamas Covenant (1988) Yale Law School - Lillian Goldman Law Library. http://avalon.law.yale.edu/20th_century/hamas.asp.

[22] https://www.state.gov/j/ct/rls/other/des/123085.htm.

[23] Profile: Hamas Palestinian Movement (May 12, 2017) BBC. https://www.bbc.com/news/world-middle-east-13331522.

[24] J. Khoury (June 10, 2017) For Arab World, Hamas Is 'Legitimate Resistance Movement,' Not Terror Group, Qatar Says. Haaretz. https://www.haaretz.com/middle-east-news/palestinians/qatar-hamas-is-legitimate-resistance-movement-1.5482546.

[25] J. Ferziger (November 14, 2018) Hamas. Bloomberg. https://www.bloomberg.com/quicktake/hamas

[26] *"Hamas also takes a hefty cut from the Egyptian tunnel trade, imposing high "customs" duties and a daily fee on local tunnel contractors. Such trade has been dramatically reduced since June 2010, when Israel quadrupled the number of trucks permitted to bring goods to Gaza through legal terminals. To replace lost tunnel income, Hamas is reportedly taking advantage of the relative drop in prices on goods arriving via official Israeli channels, imposing new taxes on various items. For example, from early July to September 20, 2010, the group barred the importation of new cars from Israel until the taxation issues were resolved."* E. Year, E. Ofer (January 6, 2011) *Gaza's Economy: How Hamas Stays in Power*. The Washington Institute. https://www.washingtoninstitute.org/policy-analysis/view/gazas-economy-how-hamas-stays-in-power.

[27] E. Year, E. Ofer (January 6, 2011) *Gaza's Economy: How Hamas Stays in Power*. The Washington Institute. https://www.washingtoninstitute.org/policy-analysis/view/gazas-econo-

ships and private wealthy benefactors[28]as, for example: funding, weapons, and training from Iran[29]; donations from the Palestinian global diaspora; fundraising (and propaganda) activities in Western Europe and North America through global charities[30] affiliated with Hamas, which collect donations on its behalf.[31]

2.2 Hamas is calling for Bitcoin donations: the rules have changed

In economic terms, Hamas is finding itself pushed to the limit, facing unprecedented financial isolation due to banking bans against the Gaza Strip by Israel and the United States, while Iran is having financial trouble due to US sanctions. Even though Israel has allowed a $15 million monthly transfer from Qatar to the Gaza Strip in the framework of new understandings reached by Israel, Egypt, and Hamas, the terrorist group is still searching for more money to fund its activities[32].

Between these events, Abu Obeida calls for bitcoin donations to support Hamas.

Basing on the documented cases of jihadists' use of cryptocurrencies[33], in less than a week after making its e-wallet address, Hamas Bitcoin donation campaign has brought a radical change in this field.

The primary element able to turn cryptocurrencies from an experimental to a consolidated terrorism financing method, is an "institutional" approval coming from influent jihadist actors (e.g. extremist Islamic scholar or leaders of an international terrorist organization).

my-how- hamas-stays-in-power.

[28] BUREAU OF COUNTERTERRORISM AND COUNTERING VIOLENT EXTREMISM (2016) *Country Reports on Terrorism*. US Department of State. https://www.state.gov/j/ct/rls/crt/2016/272235.htm.

[29] Country Reports on Terrorism (2008) U.S. Department of State. https://www.state.gov/j/ct/rls/crt/2007/103714.htm.

[30] (October 4, 2012) *Treasury Sanctions Two Hamas-Controlled Charities*. U.S. Department of Treasury. https://www.treasury.gov/press-center/press-releases/pages/tg1725.aspx.

[31] Report - Hamas. Counter Extremism Project. https://www.counterextremism.com/threat/hamas.

[32] R. Katsiri (February 3, 2019) *Hamas raises bitcoin donations via US crypto exchange*. Globes. https://en.globes.co.il/en/article-hamas-raises-bitcoin-donations-via-us-crypto-exchange-1001271661.

[33] D.M. Barone (2018) *Jihadists' use of cryptocurrencies: undetectable ways to finance terrorism*. Sicurezza Terrorismo e Società. http://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2018/11/Daniele-Maria-Barone-Jihadists%E2%80%99-use-of-cryptocurrencies_undetectable-ways-to-finance-terrorism.pdf.

Before Hamas call for bitcoin donations, in those cases documented since 2012, terrorism financing experiments through cryptocurrencies have always been conducted from activists at various levels or small groups but never directly from an international Islamic terrorist organization[34]. Indeed, the most relevant connections between cryptocurrency and an international terrorist organization are related only to a few cases, as the 4th issue released on October 2018 of al-Haqiqa magazine (an English-language magazine pro-al-Qaeda jihadists in Syria) asking for donations via either bitcoin or traditional currencies[35] or in the *Akhbar al-Muslimin* website, which used to publish news about Daesh, that launched an online fundraising campaign in November 2017 encouraging donations through Bitcoin[36]. Even though these two cases (as a very small number of other cases) seem to be strictly related to Daesh or al-Qaeda, none of their leaders has ever publicly encouraged the use of cryptocurrencies.

From this perspective, Hamas bitcoin donation campaign is already bringing to light some relevant elements of analysis.

The number of donations has highly increased: Hamas military wing issued via Telegram a request to donate to the organization by using Bitcoin. On January 31, 2019, it published a first virtual wallet address and a second one on February 2[37]. The bitcoin addresses provided by Hamas, to date, have already totally received 77 donations for the equivalent of $3.477,85.

It is relevant that, in the same day, also *Al-Nasser Salah al-Deen Brigades*, the military wing of the Popular Resistance Committees (a coalition of various armed Palestinian factions active since 2001 in the Gaza Strip, opposing to the conciliatory approach adopted by the Palestinian Authority and Fatah towards Israel)[38] used its Twitter account to call on the public to donate via bitcoin and

[34] D.M. Barone (October 22, 2018) Europol – Internet Organized Cyber Crime Threat Assessment 2018: new trends in the obscure sides of FinTech. ITSTIME. http://www.itstime.it/w/europol-internet-organized-cyber-crime-threat-assessment-2018-new-trends-in-the-obscure-sides-of-fintech-by-daniele-maria-barone.

[35] (October 15, 2018) 4th issue of al-Haqiqa magazine. Site Intel Group. https://ent.siteintelgroup.com/Western-Jihadists/4th-issue-of-al-haqiqa-magazine-features-interview-with-ttp-commander-promotes-password-security-and-bitcoin-donations.html.

[36] (December 6, 2017) Drive for Bitcoin Donations on an ISIS-affiliated website. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/drive-bitcoin-donations-isis-affiliated-website.

[37] (February 4, 2019) *Hamas and the popular resistance committees called on their supporters to donate money using the virtual currency bitcoin*. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/hamas-popular-resistance-committees-called-supporters-donate-money-using-virtual-currency-bitcoin.

[38] Popular Resistance Committees - Palestine. TRAC. https://www.trackingterrorism.org/group/popular-resistance-committees-palestine.

share a link of a private Telegram account in order to give assistance or explanations. The call read: "*For those who love jihad and the resistance in occupied Palestine, you can send donations through Bitcoin.*" The address shows that the group is receiving bitcoin donations since 2015 almost on a daily basis (4170 transactions) for a total amount of 863.49824685 BTC, almost $3millions.

It has to be taken into account that the Popular Resistance Committees are strong allies of Hamas and Islamic Jihad[39], meaning that the terrorist organizations may have agreed in choosing the crypto-way (with a fair degree of success) to receive donations or launder money since more than 3 years ago and that only now, given the strict sanctions against Hamas, they've been forced to go public.

There's not a Lack of technical skills: the research conducted by the Israeli blockchain intelligence startup Whitestream shows some sophisticated procedures in the donation process to the Hamas bitcoin address. Some donations come from US cryptocurrency exchange Coinbase and US trading platform Bittrex, other are connected to the Chinese cryptocurrencies exchange Binance, to a Russian cryptocurrency exchange Vilkov, and to CoinPayments, a company registered in the Cayman Islands. Furthermore, the US exchange platform Coinbase is only available in US, Canada, Australia, Singapore, and 38 European countries, but is not available in Palestine, and Israel, showing that donations are not coming only from local activists but are likely to come from Western sympathizers.

Moreover, in some cases an efficient method of money laundering has been used to transfer Bitcoin to Hamas, through coinMixer.io mixing service, a technology able to mix different addresses of digital currencies, thereby making it difficult to identify their users[40].

Then, while many of the addresses involved in the bitcoin donations to Hamas are holding a small amount of Bitcoin, others are coming from wealthy donors.

2.3 Positive and negative aspects in the near future scenario

Further developments are likely to come soon in this field. The call for donations in bitcoin made by Hamas could be the beginning of a consolidated trend in terrorism financing or an occasion to improve prosecution and investigation methods of this crime.

[39] Mapping Palestinian Politics - Popular Resistance Committees (PRC). ECFR. https://www.ecfr.eu/mapping_palestinian_politics/detail/popular_resistance_committees.

[40] R. Katsiri (February 3, 2019) *Hamas raises bitcoin donations via US crypto exchange.* Globes. https://en.globes.co.il/en/article-hamas-raises-bitcoin-donations-via-us-crypto-exchange-1001271661.

From this analysis, it is possible to highlight either negative or positive aspects.

On the one hand, due to the anonymity provided by cryptocurrencies, terrorists are now freely calling for donations. Indeed, even though exchange platforms ban their bitcoin address, it is still possible for them to create a new one in a few minutes and keep on receiving donations. Terrorist groups and their affiliates can make public donation requests by exploiting social media or encrypted chats, reinforcing their cultural sense of community among their supporters while circumventing the conventional banking system.

On the other hand, maybe Hamas is still able to explicitly make calls for donation in bitcoin due to the fact that its goal is prevalently political and not only religious or ideological. But for other Islamic terrorist groups' leaders (as in the case of al-Qaeda or Daesh) explicit public call for cryptocurrencies could still be a risky move. There's not yet a broadly shared Islamic religious justification to consider mainstream virtual currencies (as Bitcoin, Zcasch or Monero) as a Sharia-compliant mean of payment: Islamic scholars are still considering cryptocurrencies as gambling due to their high price volatility. In these terms, their exploitation for jihadist purposes is not fully justified by the whole Islamic community, and their use could be leverage for de-radicalization and counter-narratives able to expose their economic and geopolitical "holy war".

3. Rejecting government and banking control: alt-right extremist groups, ethno-nationalism, and anarcho-capitalism

As explained by the Christchurch shooter in his manifesto, the rejection of paying taxes is defined in right extremism narrative as "*a sign of racial loyalty*". From this perspective, circumventing the tax system is depicted as a way to sustain the ethno-nationalist cause: a fight for a nation which is defined in terms of assumed blood ties and ethnicity.[41]

Indeed, before the Christchurch shooting, back in 2017, Tarrant seems to have adopted alternative methods to raise money[42], proving that, in practical terms, according to his ideology, avoid taxes to fight for his own ethnicity and

[41] UN Human Rights Office of the High Commissioner (July 2018) *Ethno-nationalism denies millions their citizenship rights - anti-racism expert*. https://www.ohchr.org/EN/NewsEvents/Pages/EthnoNationalismDeniesTheirCitizenshipRights.aspx.

[42] B. Kaye T. Allard (April 4, 2019) *New clues emerge of accused New Zealand gunman Tarrant's ties to far right groups*. Reuters. https://uk.reuters.com/article/uk-newzealand-shooting-australia-extremi/new-clues-emerge-of-accused-new-zealand-gunman-tarrants-ties-to-far-right-groups-idUKKCN1RG093.

oppose to present policies, can legitimize the exploitation of cryptocurrencies and, in some cases, defraud other people.

Even though the references throughout his manifesto indicate that he was mostly immersed in white nationalist internet forums[43], it is important to understand that, through his extremist angle, it is possible to draw a pattern of how white supremacist narrative can change the way people perceive the world around them causing an infinite number of possible outcomes. Violent acts, exploitation of unregulated financing systems, scams.

It is fundamental to take a step back in order to explain and understand the nexus between his views, ethno-nationalism, and the exploitation of anonymous and alternative economic resources.

3.1 The extremist and illicit side effects of defending ethnicity by mocking patriotism

A key part of the extremist ideology expressed on Tarrant's manifesto is related to the increasing and irreversible weakening of white people that, according to him, is caused by unjustified welfarism of governments towards foreign cultures. From this perspective, the incapacity of politicians of protecting average hardworking white people from economic and cultural threats posed, in particular, by immigrants and ethnic minorities[44], is causing a sort of "white genocide".

This point of view is the result of a political line of thought that is growing across Western countries,[45] which is shifting states border control or clash of civilizations from an issue related to State security to a matter of personal security, turning white people into victims or directly responsible for the loss of control over the perceived irreversible and spreading disappearance of white people's national identities[46].

[43] D. Kirkpatrick (March 15, 2019) *Massacre Suspect Traveled the World but Lived on the Internet*. The New York Times. https://www.nytimes.com/2019/03/15/world/asia/new-zealand-shooting-brenton-tarrant.html.

[44] Counter Extremism Project (2018) *European Ethno-Nationalist and White Supremacy Groups*. https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/European_Ethno-Nationalist_and_White_Supremacy_Groups_081618.pdf.

[45] A. Shalal (June 24, 2018) *Migration fight erodes support for German conservatives, far-right AfD gains*. Reuters. https://www.reuters.com/article/us-germany-politics/migration-fight-erodes-support-for-german-conservatives-far-right-afd-gains-idUSKBN1JK0HV.

[46] The Economist (March 21, 2019) *Why white nationalist terrorism is a global threat*. https://www.economist.com/international/2019/03/21/why-white-nationalist-terrorism-is-a-global-threat.

Indeed, as explained by the sociologist and anthropologist Anthony D. Smith: **ethno-nationalism, is a devotion to the ethnically defined nation**, as opposed to patriotism that invokes allegiance to the territorial state.[47]

Indeed, ethno-nationalism can be merged and fuelled with a widespread sentiment of individual responsibility or victimhood towards the perception of a lack of security, subsequently causing a feeling of an imminent call-to-action against the oppressing cultures. This feeling of individual responsibility is founded on the libertarian concept of **self-interest** (either in terms of ethnicity/heritage or in terms of private property) which, taken in absolute terms, can't really provide instructive rule of thought simply because, according to this principle, each person is free to achieve in any possible way what is in their best interest. It incites people to fight for their right to "be free to exercise complete control over their own person and property"[48] thus, even discriminating or fighting against foreign cultures can be interpreted as an essential right of any property owner.

3.2 A Decentralized currency for a Decentralized order

Then, the exacerbation of the idea of a nation founded exclusively on blood-ties and cultural heritage is able to depict current governments and politicians which are not able to provide any support to defend their people from foreigners physical and cultural assault, as useless bureaucrats, liars, and enemies.

As a consequence, the tax system and banking system become an unforgivable fraud against white people.

This vision of night-watchmen State (that should serve people only by defending them in the age of crisis)[49] whose alleged legal framework recognizes sovereignty of the individual, rejects the idea of a centralized state encompassing the political philosophy of **anarcho-capitalism** by embracing the utopia of establishing a free market: self-ownership, private property and free markets at the very basis of a society able to self-regulate and civilize through the spontaneous and organic discipline of the free market. Decentralize and privatize law enforcement, courts and all other security services which would

[47] A.D. Smith (2009) Ethno-symbolism and nationalism. Routledge (108-109).

[48] J. Ganz (September 19, 2017) Libertarians have more in common with the alt-right than they want you to think. The Washington Post. https://www.washingtonpost.com/news/posteverything/wp/2017/09/19/libertarians-have-more-in-common-with-the-alt-right-than-they-want-you-to-think/?utm_term=.1d9d3ac77b22.

[49] G. Iggers (1970) *The Cult of Authority: The Political Philosophy of the Saint-Simonians.* The Hauge Martinus Nijhoff (73-75).

be selected by consumers rather than centrally controlled by a government through confiscatory taxation[50].

Against this backdrop, Richard Spencer in 2017 claimed on his Twitter profile that "*Bitcoin is the currency of the alt-right*". Decentralized, anonymous (even though governments are increasing monitoring procedures on cryptocurrency transfers)[51], and detached from the banking and tax systems, many of the members and representatives of alt-right and neo-nazi groups[52] were early adopters and many of them cashed in as the currency's valuation rose in 2017[53]. With all the data collected so far, it is a truism that extremist white supremacist groups have understood how to capitalize on the exponential rise in the value of cryptocurrencies.[54]

As in the case of **Corey D. Wilson**, who gained notoriety for promoting the spread 3D printed guns, funding Hatreon, a website that allowed neo-Nazis, white nationalists, and other extremist figures to solicit crowdfunding online, and for being named by Wired magazine[55] one of the 15 most dangerous people in the world,[56] who recently emptied his personal cryptocurrency accounts and one related to his business, Defense Distributed, totaling almost $1million[57].

[50] H. Binswanger (January 24, 2014) *Sorry Libertarian Anarchists, Capitalism Requires Government*. Forbes. https://www.forbes.com/sites/harrybinswanger/2014/01/24/sorry-libertarian-anarchists-capitalism-requires-government-2/#6cb1ad7c7d89.

[51] S. Chandler (October 07, 2018) Government Tracking of Crypto Is Growing, But There Are Ways to Avoid It. CoinTelegraph. https://cointelegraph.com/news/government-tracking-of-crypto-is-growing-but-there-are-ways-to-avoid-it.

[52] M. Bell (December 19, 2016) Meet the identitarians, Europe's 'new right'. PRI Public Radio International. https://www.pri.org/stories/2016-12-19/meet-identitarians-europes-new-right.

[53] SPLC Southern Poverty Law Center. https://www.splcenter.org/bitcoin-and-alt-right.

[54] J. Ebner (January 24, 2018) The currency of the far-right: why neo-Nazis love bitcoin. The Guardian. https://www.theguardian.com/commentisfree/2018/jan/24/bitcoin-currency-far-right-neo-nazis-cryptocurrencies.

[55] Wired magazine (December 19, 2012) *The 15 most dangerous people in the world*. https://www.wired.com/2012/12/most-dangerous-people.

[56] L. Beckett (September 19, 2018) *Gun rights activist Cody Wilson charged with sexual assault of teen*. The Guardian. https://www.theguardian.com/us-news/2018/sep/19/cody-wilson-3d-guns-sexual-assault-texas.

[57] Hatewatch Staff (September 20, 2018) *Notorious crypto-anarchist and antigovernment extremist Cody Rutledge Wilson left the country on a flight to Taiwan after he was alerted of an impending investigation against him for his alleged sexual assault of a minor.* SPLC Southern Poverty Law Center. https://www.splcenter.org/hatewatch/2018/09/20/cody-wilson-lam-1-million-bitcoin.

3.3 Not only politics and philosophy but a head for business and popularity

The use of cryptocurrencies by far-right and neo-nazi groups is not at all only related to ideologies rooted in free-market, and aversion to the political establishment.

Indeed, far-right groups became more and more interested in bitcoin as its members were **cut off from more conventional payment channels**[58]: online payment services Paypal and Apple Pay stopped transactions and froze accounts belonging to organizations and right-wing extremist activists[59].

For instance, in 2017 the Austrian Identitarian Movement, Identitäre Bewegung Österreichs (IBÖ) which is part of a larger far-right Identitarian movement with branches in most Western European countries, North America and New Zealand (the group was calling for "Remigration" for European citizens with migrants background or non-white skin, spreading fear of a great replacement a few days after Christchurch shooting[60]) and their most famous leader, Martin Sellner (who counts over 90,000 YouTube subscribers and 16,000 followers on Telegram), have increasingly been campaigning for bitcoin donations.

Furthermore, recent investigations have led Austrian police to claim that Martin Sellner, received the equivalent of €1.500 donation in bitcoin from someone whose name was Tarrant[61].

Indeed, back to Tarrant's manifesto, he explains that he worked for a short time before making some money investing in BitConnect, an open-source cryptocurrency and a peer-to-peer payment protocol.

If it was true, he didn't raise money by investing in cryptocurrencies, but by defrauding other people by becoming part of a Ponzi scheme (an illegal scam in which belief in the success of a non-existent enterprise is fostered by the payment of quick returns to the first investors from money invested by lat-

[58] D. Gerard (March 19, 2019) *Neo-Nazis Bet Big on Bitcoin (And Lost)*. Foreign Policy. https://foreignpolicy.com/2019/03/19/neo-nazis-banked-on-bitcoin-cryptocurrency-farright-christchurch.

[59] M. Steinau (January 11, 2018) *How neo-Nazis and right-wing extremists profit from bitcoin*. Business Insider. https://www.businessinsider.com/neo-nazis-and-right-wing-extremists-profit-from-the-bitcoin-hype-2018-1?IR=T.

[60] J. Ebner (April 4, 2019) *Who are Europe's far-right identitarians?*. Politico. https://www.politico.eu/article/who-are-europe-far-right-identitarians-austria-generation-identity-martin-sellner.

[61] J. Wilson (March 28, 2019) *With links to the Christchurch attacker, what is the Identitarian Movement?* The Guardian. https://www.theguardian.com/world/2019/mar/28/with-links-to-the-christchurch-attacker-what-is-the-identitarian-movement.

er investors) that has been exposed in early 2018[62]. In fact, BitConnect was a fraudulent cryptocurrency that at its height in 2017 was worth approximately $2.5 billion but that after a chain of events that started with state securities regulators sending cease-and-desist letters to the company for fraud, led to the end of the project and a totally worthless cryptocurrency[63].

3.4 Connecting the dots

According to the elements that have been documented so far there are three main aspects that can be highlighted and accurately be monitored:

- As highlighted in the case of Hamas, bitcoin still allows to detect and gather clear information about any transactions and all e-wallet connected to any suspicious donation (as happened with the suspects of Tarrant's donation to IBÖ). On the other hand, there are many other cryptocurrencies, as Monero or Zcasch, which are competing more and more on providing the most privacy-centric product, becoming digital-currencies barely traceable.
- Extremist far-right movements are trying to push their communication efforts towards a target represented by young millennials, which are usually already cyber-literate and able to master new technologies very fast. In this context, introduce brand new privacy-centric cryptocurrencies to donate money could be a very easy and quick process.
- As in the case of BitConnect, cryptocurrencies, being uncontrolled nor regulated by any sort of institution or authority, represent a fertile ground for scammers. The idea of pursuing self-interest by circumventing governments could encourage activists and sympathizers of far-right groups to look for quick profit by defrauding internet users
- Focusing on the right to exercise complete control over their own person and property, as in the case of Corey D. Wilson's 3D printed guns, it is easy to connect cryptocurrencies to dark web illegal markets, in order to spread the use of unauthorized weapons.
  This may represent the most crucial aspect: the shift from a virtual/financial threat to a physical uncontrolled threat.

[62] G. Terzo (March 15, 2019) *Christchurch Terrorist Invested and Profited from Crypto Scam Bitconnect*. CCN. https://www.ccn.com/christchurch-terrorist-invested-and-profited-from-crypto-scam-bitconnect.
[63] BitConnect value https://coinmarketcap.com/it/currencies/bitconnect.

4. Small and independent jihadist groups: The Malhama Tactical Team

The Malhama Tactical was founded in May 2016, by **Abu Rofiq** (an Arabic pseudonym that means father of Rofiq), a 24-year-old Uzbek who was killed in a Russian airstrike on February 2017. The group is known as the first private military contractor team working exclusively for extremist groups and the first one operating on Syrian soil. It consists of more or less ten well-trained fighters from Uzbekistan and the Muslim-majority republics of the Russian Caucasus.

The team has been contracted to fight, provide training, and other battlefield consulting by groups like the *Hay'at Tahrir al-Sham*, also known as al-Qaeda in Syria.

Since 2016, the Malhama Tactical has been characterized by a strong presence on social media, video sharing platforms, and encrypted chats as Telegram, Facebook, Twitter, and YouTube. Before his death, Abu Rofiq used to post videos showing the group's training courses or, covering his face by wearing a scarf, he used to describe Malhama Tactical's ongoing jobs and future projects.

The group also placed job ads on Facebook, looking for recruits who were willing to "constantly engage, develop, and learn" and join a "fun and friendly team" with vacation allowance and a day off per week.

During an interview that the former leader of the military team released via Telegram to Foreign Policy[64], he explained that Malhama Tactical was willing to take work wherever Sunni Muslims were oppressed as in China, Myanmar or North Caucasus to continue fighting against the Russian government.

After Abu Rofiq's death, the online presence of the group has been reduced for a while, until the group's new commander, **Abu Salman Belarus**, a year ago, made his first public appearance on social media.

The new leader had even more followers than his predecessor, and used to translate his messages in English, Turkish and Russian (which was the only language used by the previous leader) and now is even planning to learn French.

Abu Salam Belarus, in an interview released on Telegram to the European Eye on Radicalization[65] between July and August 2018, explained that Malhama Tactical is "primarily instructing insurgents in battle tactics, giving medical aid, working with armoured vehicles, mortars, sniper activity, and weapons

[64] R. Komar, C. Borys, E. Woods (February 10, 2017) *The Blackwater of Jihad*. Foreign Policy https://foreignpolicy.com/2017/02/10/the-world-first-jihadi-private-military-contractor-syria-russia-malhama-tactical.

[65] P. Van Ostaeyen, N. Hauer (September 19, 2018) *Interview with Abu Salman Belarus, Military Leader of Malhama Tactical*. European Eye on Radicalization. https://eeradicalization.com/interview-with-abu-salman-belarus-military-leader-of-malhama-tactical.

modifications" and that they are currently "teaching fighters of HTS (*Hay'at Tahrir al-Sham*, also known as al-Qaeda in Syria) and other groups". He also said that "quite a few of our students have become instructors, already working independently in different places".

3.1 Bitcoin donations campaign

The Malhama Tactical, being the first jihadist private military contractor, has explicitly turned the jihad into a for-profit belief. Abu Salam Belarus on Twitter, among other contents, used to call quite often for **donations in Bitcoin**. Despite the very frequent donation requests, the Bitcoin address provided by the group only received the equivalent of more or less $50. After this awkward attempt to raise money, Abu Salam Belarus deleted all the tweets calling for Bitcoin donations, inviting his followers to contact him in private to receive the Bitcoin address to give financial aid.

Even though the group, in economic terms, is not relying only on Bitcoin, the case of the Malhama Tactical is relevant to either consolidate some of the information gathered so far or provide new elements to analyse the jihadists' use of cryptocurrencies.

– **A clear militaristic intent instead of a politically correct approach**
  Jihadist donation campaigns asking for cryptocurrencies are explicitly aimed at providing supplies, training facilities, and weapons for the mujahideen. A kind of communication strategy very different from those campaigns, remotely linked to a terrorist organization, calling for donations through the conventional banking system and usually disguised behind charitable or religious intents. The shift into a more explicit message is likely to be allowed by the anonymity provided by the blockchain or digital ledger technologies[66].

– **The limited use of cryptocurrencies is not always related to a lack of technical skills**[67]
  Cryptocurrencies, Bitcoin in particular, are becoming a mainstream asset in legal markets. In fact, over time, their use is requiring less and less technical skills, causing an expansion of their catchment area

[66] International Institute on Counter-Terrorism *Trends in Cyberspace*. IDC Herzliya – International Institute for Counter-Terrorism (ICT). https://www.ict.org.il/Article/2230/Trends_in_Cyberspace_Annual_Summary_2017#gsc.tab=0.

[67] S. Webb (November 23, 2018) *Market blow up - ISIS war chest decimated by Bitcoin crash after terror chiefs invested millions in collapsing cryptocurrency, an expert claims*. The Irish Sun. https://www.thesun.ie/news/3424201/isis-war-chest-decimated-by-bitcoin-crash-after-terror-chiefs-invested-millions-in-collapsing-cryptocurrency.

which is also reaching terrorist supporters. Indeed, jihadist donation campaigns calling for cryptocurrencies are increasing in numbers since 2012[68]. Nevertheless, many legal users (and also jihadist supporters and religious leaders) are being sceptical about cryptocurrencies, due to the risks related to their price volatility and, for the same reasons, they are not yet spreading as a broadly exploited instrument for terrorism financing. But these concerns are only keeping Islamic terrorists from using cryptocurrencies as a store of value, not from exploiting them to move small or big amounts of money in complete anonymity and in a short range of time. In these terms, FinTech sector is allowing the creation of a potential, faster, substitute of the *hawala* system.[69]

– **One man's terrorist is another man's freedom fighter**
It is a truism that propaganda and communication are able to strengthen Islamic terrorists' narrative, turning a small group using violence and religion to raise money, into an army bravely fighting against the *takfir* (infidels). The truth is that, behind the narrative and storytelling depicting a courageous leader who is defeating an oppressive regime, there is a global strategy aimed at getting the world attention. Freedom, self-determination and religion, added to an online friendly Western communication strategy (e.g. job ads or business-oriented catchy advertisements) are the pillars of this new type of jihadist brand.
Hence, even though calls for anonymous donations through cryptocurrencies are still explicitly militaristic, jihadist groups are always hiding behind lies, trying to represent themselves as romantic and appealing young warriors fighting in the name of liberation. But there's no liberation in their intent. There's only an oppressive, colonialist, and violent will that groups as Malhama Tactical, despite being very small, are promoting, financing, and fuelling with bloodshed.

[68] E. Azani N. Liv (January 30, 2018) *Jihadists' Use of Virtual Currency*. IDC Herzliya – International Institute for Counter-Terrorism (ICT). https://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pdf.
[69] ITSTIME (June 7, 2018) *Bitcoin and other types of cryptocurrency: modern and undetectable ways to finance terrorism*. http://www.itstime.it/w/bitcoin-and-other-types-of-cryptocurrency-modern-and-undetectable-ways-to-finance-terrorism-by-daniele-maria-barone.

4. Suspicious humanitarian crowdfunding campaigns in bitcoin and their exploitation of exchange services.

The world's attention to the war in Syria is allowing jihadist groups to change their narrative, by disguising their intents also behind a false image built around humanitarian aid or struggle against war criminals oppressing innocent people.

This is potentially giving terrorist organizations and their sympathizers the chance to widen the heterogeneity of their affiliates by globally leveraging through the internet on the atrocities and injustice brought by the war, overlapping issues exclusively concerning violent extremism or radicalization.

In economic terms, this branch of the global jihadist web communication strategy is translating into a growing number of apparently decentralized (i.e. carried out by individuals or small groups) crowdfunding campaigns accepting bitcoin for either explicit militaristic or charity purposes as in the case Isis suspects in Al-Hol camp raising money through online crowdfunding campaign[70].

These campaigns are very numerous and are generating more and more difficulties either in how to identify their real intent (if terrorist related or just scams) and in tracking down the total amount of funds received.

Indeed, on Telegram, these calls for donations are usually only advertised by explicit jihadist chat groups without ever interacting directly with them; create mirror groups to avoid the risk of being blocked or tracked; provide several donation methods (e.g. PayPal, fundraising platforms on the public web, various bitcoin addresses).

In order to better explain this trend, the following analysis will focus on a few topic cases related to this opaque calls for bitcoin, as **Sadaqa al-Kahir** and **al-Ikhwa**, self-proclaimed charity groups aimed at giving aid in Syria, and **al-Sadaqa**, a jihadist campaign raising money to support the mujahideen and some of the bitcoin addresses and transactions processed to finance these groups.

4.1 Binance bitcoin address (...*bu1s*)

Before deepening into the analysis of these campaigns, is worth doing a short explanation on the bitcoin address "...*bu1s*" (last four characters of the bitcoin address), which is where the most majority of the donations that will be traced are sent.

[70] R.Hall (July 25, 2019) *Isis suspects in Syrian camp raise thousands through online crowdfunding campaign*. The Independent. https://www.independent.co.uk/news/world/middle-east/isis-syria-camp-al-hol-paypal-telegram-online-crowdfunding-a9021006.html.

As explained by Bellingcat[71] and Cointelegraph[72], this address belongs to **Binance**, a very well-known crypto exchange service, which allows users to trade cryptocurrencies for fiat money or other digital currencies. In particular, it was discovered that this exchange service has been used to send bitcoin to *Izz ad-Din al-Qassam Brigades*, the military wing of Hamas[73].

This doesn't mean or proves at all a direct implication of the exchange service in terrorism financing, but it only means that these funds have been exchanged (after a few steps) into cash or other digital currencies by exploiting Binance.

The transactions of these campaigns, usually, before reaching Binance bitcoin address, made a donation to other bitcoin addresses. These bitcoin addresses may belong either to other exchange services working as middlemen between the crowdfunding campaign and Binance or could belong to a mixing service (to disguise the sender and the receiver)[74], to launder and hide the bitcoin donated before being cashed through Binance, or could also belong to private parties involved in this pattern.

Below, a description of each campaign and of some of the most significant transactions analysed.

4.2 Al-Sadaqah Donation Campaign (... *Nwpf*, ...*qLez*)

Since November 2017 a*l-Sadaqah* (the charity) organization, began a still ongoing fundraising campaign on Telegram, other social media such as Twitter, and on the deep web[75] to raise bitcoin from Western supporters. The explicit intent of the call for bitcoin is to finance the *mujahideen* fighting against the Assad regime in north-eastern Syria[76]. Nowadays, the organization's Twitter page has been shut down, but its English and French Telegram accounts are still online.

[71] B. Smith (March 26, 2019) How To Track Illegal Funding Campaigns Via Cryptocurrency. Bellingcat. https://www.bellingcat.com/resources/how-tos/2019/03/26/how-to-track-illegal-funding-campaigns-via-cryptocurrency.

[72] https://cointelegraph.com/news/binance-vs-mcafee-hack-rumors-refuted-cryptocurrency-trading-resumed.

[73] D.M. Barone (February 06, 2019) Hamas crowdfunding bitcoin: legitimizing cryptocurrencies from a jihadist perspective. ITSTIME http://www.itstime.it/w/hamas-crowdfunding-bitcoin-legitimizing-cryptocurrencies-from-a-jihadist-perspective-by-daniele-maria-barone.

[74] https://cryptalker.com/bitcoin-mixer.

[75] http://cjlab.memri.org/latest-reports/online-campaign-in-english-raising-funds-for-the-jihad-in-syria-in-bitcoin.

[76] http://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2018/11/Daniele-Maria-Barone-Jihadists%E2%80%99-use-of-cryptocurrencies_undetectable-ways-to-finance-terrorism.pdf.

The campaign seems not to be very popular. The BTC address advertised on *al-Sadaqah*, "...*Nwpf*", shows that from November 2017 until its last donation on October 28, 2018, has received an amount equivalent to more or less $1,000 and processed 8 transactions (4 inputs and 4 outputs). Although most of the transfers were only worth a few dollars, one Bitcoin wallet from which a transaction was made to the wallet of Al-Sadaqa stood out ...*85oC*, which has totally received the equivalent of more or less $7millions.[77] This Bitcoin wallet was associated with the kidnapping of a child in South Africa in May 2018 and many frauds.[78]

The wallet linked to the jihadist donation campaign[79] includes also another address "...*qLez*" (total received roughly $150).

Going backward from the only one donation received by this address, it appears that small amount of bitcoin (a few hundred dollars) has been transferred from one bitcoin address to another and all of them have only one input and one output. The interesting data is that the more we go back to the source of the only donation made to ...*qLez*, the more we encounter an increasing number of wealthy bitcoin addresses (as *FkdG*), worth the equivalent of thousands of hundred dollars.

Given that these addresses belong to e-wallets with only one bitcoin address[80], they're likely to belong to private wealthy donors rather than to any crypto-exchange or trading platform.

About the outputs of al-Sadaqa BTC addressees, the amount of bitcoin that their call for donations raised has been donated in full and, 4 out of these 5 outputs, as to "...*nbQ*" - "...*WFDD8*" - "...*Xt6D*", carry out the same method to send their bitcoin to Binance wallet address:

- They periodically receive small amounts (from a few hundred to $1.500) from different BTC addresses.
- Then, that same day or the very next day, they do a multiple input transaction: send the small amount received to another bitcoin address and a larger amount (until $1 million) always to "...*bu1s*", i.e. Binance (the big orange dot in the picture below).

These first wallets, where the donations are directly made by al-Sadaqa, could not belong to any private receiver but, given the incredible amount

[77] N. Liv (July 2019) Jihadists' Use of Virtual Currency 2. International Institute for Counter Terrorism ICT. https://www.ict.org.il/images/Jihadists%20use%20of%20virtual%20currency%202.pdf.
[78] B. Strick (June 18, 2018) Tracing a Jihadi cell, kidnappers and a scammer using the blockchain – an open source investigation. Medium. https://medium.com/@benjamindbrown/tracing-syrian-cell-kidnappers-scammers-finances-through-blockchain-e9c52fb6127d.
[79] https://www.walletexplorer.com/wallet/ae0f2ea8de2764e9/addresses.
[80] https://www.walletexplorer.com/wallet/6402b0d863591976/addresses.

of bitcoin addresses owned by their e-wallets, are very likely to belong to an exchange platform or a bitcoin tumbler (a mixing service).

4.3 Humanitarian aid requests advertised on independent jihadist Telegram groups: al-Khair charity group and al-Ikhwa

As previously mentioned, not only explicit jihadist campaigns are calling for bitcoin donations for Syria, but also independent self-proclaimed charity groups.

Al-Ikhwa (The Brothers) and Sadaqa al-Khair present themselves as non-profit organizations, which are collecting donations to help the Syrian population, soliciting money also via Bitcoin to support widows and orphans.[81]

They both made their first appearance on Telegram more or less one year ago, posting extreme war images and video, in English and German, of armed attacks against civilians and of their initiatives to give aid to the Muslim people in Syria. Furthermore, both of these crowdfunding humanitarian campaigns declare on their Telegram and Facebook pages that they prefer to use alternative and anonymous fundraising methods because the conventional banking system or non-anonymous ways to receive and call for donations are already preventing them from processing any sort of payment (i.e. donorbox.com or wire transfers). Indeed, in order to help the needy and avoid authorities controls, they're calling for donations via Paypal, money transfers, some crowdfunding platform on the clear web, and also in bitcoin.

Both of these charity campaigns have been advertised by Telegram chat groups which post explicit jihadist material, that have sponsored bitcoin donations to help the mujahideen by supporting military groups and crowdfunding campaigns as the **Malhama Tactical Team** (private military contractor team working exclusively for jihadist groups)[82] and **SadaqaCoins** (a cryptocurrencies crowdfunding website on the deep web, aimed at funding the mujahideen in Syria).[83] Even though most of these groups have among a few hundred to 2000 subscribers, their contents have been viewed by thousands of users. Some of these Telegram groups also promote the **use of bitcoins by**

[81] https://www.memri.org/jttm/charity-group-telegram-solicits-money-bitcoin-%E2%80%8Esupports-syrian-fighters-wives-martyrs%E2%80%8E.

[82] D.M. Barone (December 01, 2018) Jihad as a Business Segment: the Malhama Tactical Team. ITSTIME. http://www.itstime.it/w/jihad-as-a-business-segment-the-malhama-tactical-team-by-daniele-maria-barone.

[83] N. Liv (July 2019) Jihadists' Use of Virtual Currency 2. International Institute for Counter Terrorism ICT. https://www.ict.org.il/images/Jihadists%20use%20of%20virtual%20currency%202.pdf.

sharing self-made user's manuals and explain the reasons why it is right to **use cryptocurrencies according to the Sharia**.

In terms of donations, it seems that this communication strategy is already paying off.

4.4 Sadaqa al-Khair charity group: ...*51u7*

In a few days (from May 21, 2019, until May 30, 2019) al-Khair BTC address ...*51u7*, at the time of writing, shows a total of 6 transactions (3 inputs and 3 outputs) and a total received of more or less the equivalent of $1,100.

After a few days, the charity group didn't publicly provide anymore its bitcoin address. Thus, it is possible that they're providing a new bitcoin address on a private chat in order to avoid being detected.

All of the funds received have been transferred to other bitcoin addresses ...*MUaC* (once) and ...*pXai* (twice).

Also, in this case, there is a common pattern which leads to ...*bu1s*, Binance, very similar to the one seen in al-Sadaqa, adding a few steps more.

In fact, the donations made by the al-Khair charity group, are firstly passing through two or three brand new BTC addresses, with two transactions each, at most, in order to be subsequently transferred to wealthier wallets which in the end move their funds to ...*bu1s* (the big orange dot in the picture below).[84]

Same as in al-Sadaqa, the transfers involving BTC addresses which seem to be owned by private donors is made in the first or the second step of this chain. Thus, it is more likely that the wealthiest bitcoin wallets involved in these specific donations already belong to Binance or to another exchange service/mixing service which uses Binance to exchange cryptocurrencies. Hence, it seems that this campaign is not directly involving any wealthy donor.

4.5 Al-Ikhwa Independent Charity (several BTC addresses)

The al-Ikhwa crowdfunding campaign is using different bitcoin public addresses that, after the first four months of activities (since November 2018), have been monthly updated on their Telegram group in rotation. (...*6p6S* ...*Vgea* ...*zcHH* ...*deKc* ...*8ELo* ...*AU5j* ...*XLRs* ...*zXyz* ...*zcHH*).

Starting since July 2018 the self-proclaimed charity group has received, ignoring non-public bitcoin addresses provided only through the private chat, a total amount of more or less $3000. The charity campaign received its first donation on ...*zcHH* on March 2019 and the last donations have been received at the beginning of June 2019.

[84] https://www.blockchain.com/it/btc/tree/453240296.

Many of these addresses belong to the same bitcoin wallet[85], and in some cases have been used to send a multiple inputs (a donation made simultaneously from different bitcoin addresses to one or many other wallets) of more or less totally $700 to ...*wwxi*.[86]

This donation was then split into two different transactions: one is more likely to already belong to an exchange service/mixing service (its wallet has 108.496 total addresses) and then transferred to ...*bu1s*.

Then, the other donation was sent to another bitcoin address with a total amount received of $200 in 1 input and 1 output which then repeated the same process seen before to reach Binance bitcoin address[87] (the bigger orange dots in the picture below).

This process is repeated in almost all the bitcoin transferred by al-Ikhwa campaign to other bitcoin addresses until Binance.

As opposed to Hamas bitcoin crowdfunding campaign, in these cases the exploitation of Binance is related to the final output, meaning that the money received could be directly exchanged or used to finance other e-wallets.

This analysis explained the modus operandi of only a very limited number of the BTC addresses involved in these crowdfunding campaigns. Indeed, there are many others either wealthy or relatively poor addresses operating through this pattern, which bring out a very complex and solid network.

Hence, it is possible to highlight the following main aspects:

– Opaque humanitarian calls for anonymous donations may increase the difficulty to evaluate if there's a nexus between their charity fundraising campaigns and terrorism financing by making more and more unclear which one is reliable (e.g. moved by a legitimate purpose) or connected to a jihadist group (as a smokescreen to disguise terrorism financing or money laundering) or just a major scam. In the cases of Sadaqa al-Khair and al-Ikhwa, being advertised and supported by explicit jihadist Telegram chat groups could mean both that they support a jihadist group and that they are just a fraud. In both cases, the fact that they are able to freely ask, send and receive bitcoins should be stopped just in the same way it already happens when they try to exploit the conventional banking system or public and legitimate crowdfunding websites.

[85] https://www.walletexplorer.com/wallet/3bfee78719643a94/addresses.

[86] https://www.blockchain.com/it/btc/tx/7ad7c55e8724e9db3ca54651a3d7ab0591c93ce2bc0e5c39f97d09f09df8cc7d.

[87] https://www.blockchain.com/it/btc/tree/431361274.

– Crowdfunding campaigns as al-Sadaqa, al-Khair and al-Ikhwa don't seem to have received huge amounts of bitcoin but this doesn't necessarily mean that they can't be a part of a wider network. Cases like these are becoming more and more frequent since 2017: they ask for bitcoin in order to help the Muslim Syrian population either by arming them to fight against the Assad and Western governments or by giving aid to the orphans or widows; they receive an amount in bitcoin in a range from roughly $1.000 to $3.000; they usually operate for more or less a year. They could act as digital-money mules or bitcoin tumblers, transferring from time to time small amounts of bitcoin through an infinite number of e-wallets, in order to let wealthy jihad supporters to be disguised and act unopposed while moving huger amounts of wealth globally and anonymously through them. In this case, they could have the double role of being a smokescreen (able to hide wealthier transactions) and a fundamental tactical role in facilitating terrorism financing.

5. Summary

The most recent developments in the cryptocurrency/violent extremism ecosystem are highlighting, on the one hand, how a grey legal framework in the FinTech sector is currently keeping authorities and analysts from efficiently tracking down and prosecuting illicit financing methods, on the other hand, how the liquidity of terrorist groups strategies and tactics are constantly evolving. Moreover, as previously analysed in this essay, extremist groups are more and more becoming able to find either religious or political justifications to encourage their members or sympathizers to stay up to date on the most recent financing methods, by leveraging on their duties towards the organizations.

Focusing on the different areas and cases analysed in this essay, it is possible to understand that, even though every branch discussed has its peculiarity, they still present common denominators.

In the cases regarding the exploitation of cryptocurrencies by white supremacist groups, they are ideologically self-sustained by the refusal of a centralized economic control (e.g. taxes and policies unable to support white heritage and cultures) and the consequential will to establish an alternative source to finance, store and invest money while circumventing authorities or legal restrictions on conventional channels, increase privacy, and keep on spreading their propaganda.

Through this lens, cryptocurrencies become powerfully meaningful: a clandestine instrument to help their ethnicity. In these terms, crypto-

currencies are turned into a cornerstone of the communication strategies adopted by al-right groups.

On the contrary, in the events related to jihadist organizations as Hamas, they are overlapping the religious and ideological justification. In particular, it seems that after the first announcement made by Abu Obeida on January 29 about the incoming possibility to make donations via bitcoin to the organization, many activists and supporters have raised questions about cryptocurrencies. Indeed, the day after its first call for bitcoin, Hamas published an infographic about the Bitcoin on the Hamas-affiliated newspaper *Al-Resalah* explaining what Bitcoin is and, probably to reassure its supporters about their investment, stressing that the daily trade in bitcoin amounts is approximately $6 million, and that the total amount on the Internet is estimated at $61 billion.[88] Moreover, it is relevant that Hamas donation campaign in bitcoin is the first jihadist case in this field without any particular religious justification concerning the use of cryptocurrencies. Indeed, even though the debate about cryptocurrencies is still ongoing in the Islamic community and among Islamic scholars, it seems that, in this case, donors were prevalently worried about their investments rather than use a not yet fully recognized Sharia-compliant product as a mean of payment[89]. For Hamas it was enough to claim that "*The Zionist enemy fights the Palestinian resistance by trying to cut aid to the resistance by all means, but lovers of resistance around the world fight these Zionist attempts and seek all possible means to aid the resistance*" to convince its supporters that cryptocurrencies are a legitimate method to fund the jihad.[90]

Another important aspect is related to the diffusion of skills among these groups, which is not only regulated at an "institutional" level (e.g. violent extremist organizations leaders or endorsers) but it is autonomously also spreading through small independent clusters (as suspicious online humanitarian crowdfunding campaigns), individuals (as Tarrant), and

[88] (February 4, 2019) *Hamas and the popular resistance committees called on their supporters to donate money using the virtual currency bitcoin*. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/hamas-popular-resistance-committees-called-supporters-donate-money-using-virtual-currency-bitcoin.

[89] D.M. Barone (August 16, 2018) Cyber Jihad and Terrorism Financing: New Methods – Old Rules. ITSTIME. http://www.itstime.it/w/cyber-jihad-and-terrorism-financing-new-methods-old-rules-by-daniele-maria-barone.

[90] (February 4, 2019) *Hamas and the popular resistance committees called on their supporters to donate money using the virtual currency bitcoin*. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/hamas-popular-resistance-committees-called-supporters-donate-money-using-virtual-currency-bitcoin.

small groups (as Malhama Tactical) which are causing the diffusion of a terrorism financing maze, similar to the phenomenon happening in the illegal deep web markets described in the IOCTA 2018.

All of these elements are creating a confusing environment, which can make investigations and prosecutions on terrorism financing even more difficult.

Focusing on small crowdfunding campaigns, it is still crucial to introduce stricter and updated Anti Money Laundering and Know Your Customer (KYC) policies applied to every user who wants to exchange or purchase even small amounts of bitcoin (e.g. less than the equivalent $2000). Binance, for instance, has already updated its account verification process, with the mandatory request of providing a valuable ID (e.g. National Identification Card, Permanent Residence Card, International Passport) even though, it is still not specified if there's a minimum expense required by the user to be obliged to provide a valid document to the platform[91]. Nevertheless, there are still many others exchange or mixing services available which still don't require, at the time of writing, any information about their users to purchase, receive or send either small or big amounts of digital currencies. This current situation allows the exploitation of digital money-mules or mixing services which can still easily scramble and hide wealthy illegitimate transactions.

It has to be stressed that, besides these complications, there are positive aspects to take into account. Blockchain technology is offering an unprecedented tool for investigations: from one single suspicious transaction, it is possible to track back all the financial history of the people involved in one crime. In these terms, the use of the web for terrorist purposes is still a double-edged sword; it can surely give a strong advantage to terrorist organizations in terms of anonymity and allow them to keep on widening their range through strengthening communication and crowdfunding practices, but authorities monitoring methods are subsequently improving. Even though the current legal framework makes it difficult to prosecute the illegal exploitation of many modern online tools, as long as the internet will be the primary way for violent extremist groups or individuals to keep an international unity among their members, they will still be exposed to controls and analysis.

[91] https://support.binance.je/hc/en-us/articles/360020832652-How-to-Complete-the-Account-Verification-KYC-Process.

References

A.D. Smith (2009) Ethno-symbolism and nationalism. Routledge (108-109).

A. Shalal (June 24, 2018) *Migration fight erodes support for German conservatives, far-right AfD gains*. Reuters. https://www.reuters.com/article/us-germany-politics/migration-fight-erodes-support-for-german-conservatives-far-right-afd-gains-idUSKBN1JK0HV.

B. Kaye T. Allard (April 4, 2019) *New clues emerge of accused New Zealand gunman Tarrant's ties to far right groups*. Reuters. https://uk.reuters.com/article/uk-newzealand-shooting-australia-extremi/new-clues-emerge-of-accused-new-zealand-gunman-tarrants-ties-to-far-right-groups-idUKKCN1RG093.

Bureau of Counterterrorism and Countering Violent Extremism (2016) *Country Reports on Terrorism*. US Department of State. https://www.state.gov/j/ct/rls/crt/2016/272235.htm.

B. Smith (March 26, 2019) How To Track Illegal Funding Campaigns Via Cryptocurrency. Bellingcat. https://www.bellingcat.com/resources/how-tos/2019/03/26/how-to-track-illegal-funding-campaigns-via-cryptocurrency.

B. Strick (June 18, 2018) *Tracing a Jihadi cell, kidnappers and a scammer using the blockchain – an open source investigation*. Medium. https://medium.com/@benjamindbrown/tracing-syrian-cell-kidnappers-scammers-finances-through-blockchain-e9c52fb6127d.

Country Reports on Terrorism (2008) U.S. Department of State. https://www.state.gov/j/ct/rls/crt/2007/103714.htm.

Counter Extremism Project (2018) *European Ethno-Nationalist and White Supremacy Groups*. https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/European_Ethno-Nationalist_and_White_Supremacy_Groups_081618.pdf.

D. Gerard (March 19, 2019) *Neo-Nazis Bet Big on Bitcoin (And Lost)*. Foreign Policy. https://foreignpolicy.com/2019/03/19/neo-nazis-banked-on-bitcoin-cryptocurrency-far-right-christchurch.

D. Kirkpatrick (March 15, 2019) *Massacre Suspect Traveled the World but Lived on the Internet*. The New York Times. https://www.nytimes.com/2019/03/15/world/asia/new-zealand-shooting-brenton-tarrant.html.

D. Manheim, P.B. Johnston, J. Baron, C. Dion-Schwarz (April 21, 2017) *Are Terrorists Using Cryptocurrencies?* RAND Corporation. Available at https://www.rand.org/blog/2017/04/are-terrorists-using-cryptocurrencies.html.

D.M. Barone (2018) *Jihadists' use of cryptocurrencies: undetectable ways to finance terrorism*. Sicurezza Terrorismo e Società. http://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2018/11/Daniele-Maria-Barone-Jihadists%E2%80%99-use-of-cryptocurrencies_undetectable-ways-to-finance-terrorism.pdf.

D.M. Barone (August 16, 2018) Cyber Jihad and Terrorism Financing: New Methods – Old Rules. ITSTIME. http://www.itstime.it/w/cyber-jihad-and-terrorism-financing-new-methods-old-rules-by-daniele-maria-barone.

D.M. Barone (June 7, 2018) *Bitcoin and other types of cryptocurrency: modern and undetectable ways to finance terrorism*. ITSTIME http://www.itstime.it/w/bitcoin-and-other-types-of-cryptocurrency-modern-and-undetectable-ways-to-finance-terrorism-by-daniele-maria-barone.

E. Azani N. Liv (January 30, 2018) *Jihadists' Use of Virtual Currency*. IDC Herzliya – International Institute for Counter-Terrorism (ICT) https://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pdf.

Europol (2018) I*nternet Organised Crime Threat Assessment (IOCTA) 2018*. European Union Agency for Law Enforcement Cooperation. Available at https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.

E. Year, E. Ofer (January 6, 2011) *Gaza's Economy: How Hamas Stays in Power*. The Washington Institute. https://www.washingtoninstitute.org/policy-analysis/view/gazas-economy-how-hamas-stays-in-power.

E. Spagnuolo (April 26, 2017) Addio Bitcoin, nel deep web ora si paga con Monero e Zcash. Wired - Italia. https://www.wired.it/economia/finanza/2017/04/26/bitcoin-monero-zcash.

G. Iggers (1970) *The Cult of Authority: The Political Philosophy of the Saint-Simonians*. The Hauge Martinus Nijhoff (73-75).

G. Terzo (March 15, 2019) *Christchurch Terrorist Invested and Profited from Crypto Scam Bitconnect*. CCN. https://www.ccn.com/christchurch-terrorist-invested-and-profited-from-crypto-scam-bitconnect.

Hamas Covenant (1988) Yale Law School - Lillian Goldman Law Library. http://avalon.law.yale.edu/20th_century/hamas.asp.

H. Binswanger (January 24, 2014) *Sorry Libertarian Anarchists, Capitalism Requires Government*. Forbes. https://www.forbes.com/sites/harrybinswanger/2014/01/24/sorry-libertarian-anarchists-capitalism-requires-government-2/#6cb1ad7c7d89.

Hatewatch Staff (September 20, 2018) *Notorious crypto-anarchist and antigovernment extremist Cody Rutledge Wilson left the country on a flight to Taiwan after he was alerted of an impending investigation against him for his alleged sexual assault of a minor*. SPLC Southern Poverty Law Center. https://www.splcenter.org/hatewatch/2018/09/20/cody-wilson-lam-1-million-bitcoin.

International Institute on Counter-Terrorism *Trends in Cyberspace*. IDC Herzliya – International Institute for Counter-Terrorism (ICT) https://www.ict.org.il/Article/2230/Trends_in_Cyberspace_Annual_Summary_2017#gsc.tab=0.

J. Bohannon (March 9, 2016) Why criminals can't hide behind Bitcoin. ScienceMag. Available at http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

J. Ebner (January 24, 2018) The currency of the far-right: why neo-Nazis love bitcoin. The Guardian. https://www.theguardian.com/commentisfree/2018/jan/24/bitcoin-currency-far-right-neo-nazis-cryptocurrencies.

J. Khoury (June 10, 2017) For Arab World, Hamas Is 'Legitimate Resistance Movement,' Not Terror Group, Qatar Says. Haaretz. https://www.haaretz.com/middle-east-news/palestinians/qatar-hamas-is-legitimate-resistance-movement-1.5482546.

J. Ganz (September 19, 2017) Libertarians have more in common with the alt-right than they want you to think. The Washington Post. https://www.washingtonpost.com/news/posteverything/wp/2017/09/19/libertarians-have-more-in-common-with-the-alt-right-than-they-want-you-to-think/?utm_term=.1d9d3ac77b22.

J. Wilson (March 28, 2019) *With links to the Christchurch attacker, what is the Identitarian Movement?* The Guardian. https://www.theguardian.com/world/2019/mar/28/with-links-to-the-christchurch-attacker-what-is-the-identitarian-movement.

K. Marinos (March 23, 2016) *Are Bitcoin Transactions Traceable?*. CoinTelegraph. Available at https://cointelegraph.com/news/are-bitcoin-transactions-traceable.

L. Beckett (September 19, 2018) *Gun rights activist Cody Wilson charged with sexual assault of teen*. The Guardian. https://www.theguardian.com/us-news/2018/sep/19/cody-wilson-3d-guns-sexual-assault-texas.

Mapping Palestinian Politics - Popular Resistance Committees (PRC). ECFR. https://www.ecfr.eu/mapping_palestinian_politics/detail/popular_resistance_committees.

M. Arnold, S.A. Ramadan (January 30, 2018) *Hamas Calls on Supporters to Donate to Group in Bitcoin*. Bloomberg. https://www.bloomberg.com/news/articles/2019-01-30/hamas-calls-on-supporters-to-donate-to-group-in-bitcoin.

M. Bell (December 19, 2016) Meet the identitarians, Europe's 'new right'. PRI Public Radio International. https://www.pri.org/stories/2016-12-19/meet-identitarians-europes-new-right.

M. Levitt, D. Ross (2007) *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*. Yale University Press.

M. Steinau (January 11, 2018) *How neo-Nazis and right-wing extremists profit from bitcoin*. Business Insider. https://www.businessinsider.com/neo-nazis-and-right-wing-extremists-profit-from-the-bitcoin-hype-2018-1?IR=T.

N. Liv (July 2019) Jihadists' Use of Virtual Currency 2. International Institute for Counter Terrorism ICT. https://www.ict.org.il/images/Jihadists%20use%20of%20virtual%20currency%202.pdf.

O. Kharif (January 2, 2018) *The Criminal Underworld Is Dropping Bitcoin for Another Currency*. Bloomberg. Available at https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency.

Popular Resistance Committees - Palestine. TRAC. https://www.trackingterrorism.org/group/popular-resistance-committees-palestine.

Profile: Hamas Palestinian Movement (May 12, 2017) BBC. https://www.bbc.com/news/world-middle-east-13331522.

P. Koshy D. Koshy P. McDaniel (2014) *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*. Pennsylvania State University, University Park, PA 16802, USA. Available at https://pdfs.semanticscholar.org/c277/62257f068fdbb2ad34e8f787d8af13fac7d1.pdf.

P. Van Ostaeyen, N. Hauer (September 19, 2018) *Interview with Abu Salman Belarus, Military Leader of Malhama Tactical*. European Eye on Radicalization. https://eeradicalization.com/interview-with-abu-salman-belarus-military-leader-of-malhama-tactical.

Report - Hamas. Counter Extremism Project. https://www.counterextremism.com/threat/hamas.

R.Hall (July 25, 2019) *Isis suspects in Syrian camp raise thousands through online crowdfunding campaign*. The Independent. https://www.independent.co.uk/news/world/middle-east/isis-syria-camp-al-hol-paypal-telegram-online-crowdfunding-a9021006.html.

R. Katsiri (February 3, 2019) *Hamas raises bitcoin donations via US crypto exchange*. Globes. https://en.globes.co.il/en/article-hamas-raises-bitcoin-donations-via-us-crypto-exchange-1001271661.

R. Komar, C. Borys, E. Woods (February 10, 2017) *The Blackwater of Jihad*. Foreign Policy https://foreignpolicy.com/2017/02/10/the-world-first-jihadi-private-military- contractor-syria-russia-malhama-tactical.

S. Chandler (October 07, 2018) Government Tracking of Crypto Is Growing, But There Are Ways to Avoid It. CoinTelegraph. https://cointelegraph.com/news/government-tracking-of-crypto-is-growing-but-there-are-ways-to-avoid-it.

SPLC Southern Poverty Law Center. https://www.splcenter.org/bitcoin-and-alt-right.

S. Webb (November 23, 2018) *Market blow up - ISIS war chest decimated by Bitcoin crash after terror chiefs invested millions in collapsing cryptocurrency, an expert claims*. The Irish Sun. https://www.thesun.ie/news/3424201/isis-war-chest-decimated-by-bitcoin-crash-after-terror-chiefs-invested-millions-in-collapsing-cryptocurrency.

The Economist (March 21, 2019) *Why white nationalist terrorism is a global threat*. https://www.economist.com/international/2019/03/21/why-white-nationalist-terrorism-is-a-global-threat.

UN Human Rights Office of the High Commissioner (July 2018) *Ethno-nationalism denies millions their citizenship rights - anti-racism expert*. https://www.ohchr.org/EN/NewsEvents/Pages/EthnoNationalismDeniesTheirCitizenshipRights.aspx.

Wired magazine (December 19, 2012) *The 15 most dangerous people in the world*. https://www.wired.com/2012/12/most-dangerous-people.

(March 7, 2019) *Funding Terrorism: ISIS raises funds through an affiliated website, using bitcoins*. The Meir Amit Intelligence and Terrorism Information Center. https://www.terrorism-info.org.il/app/uploads/2019/03/E_054_19.pdf.

(February 12, 2019) *Drive for donations using Bitcoin on an ISIS affiliated website*. The Meir Amit Intelligence and Terrorism Information Center. https://www.terrorism-info.org.il/app/uploads/2019/02/E_018_19.pdf.

(February 4, 2019) *Hamas and the popular resistance committees called on their supporters to donate money using the virtual currency bitcoin*. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/hamas-popular-resistance-committees-called-supporters-donate-money-using-virtual-currency-bitcoin.

(October 15, 2018) 4th issue of al-Haqiqa magazine. Site Intel Group. https://ent.siteintelgroup.com/Western-Jihadists/4th-issue-of-al-haqiqa-magazine-features-interview-with-ttp-commander-promotes-password-security-and-bitcoin-donations.html.

(December 6, 2017) Drive for Bitcoin Donations on an ISIS-affiliated website. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/drive-bitcoin-donations-isis-affiliated-website.

(October 4, 2012) *Treasury Sanctions Two Hamas-Controlled Charities*. U.S. Department of Treasury. https://www.treasury.gov/press-center/press-releases/pages/tg1725.aspx.

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 978-88-9335-540-7

Euro 20,00