ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

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

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

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

8

ISSUE 2/2018

Milano 2018

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

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

ISSUE 2 – 8/2018

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: 978-88-9335-387-8

copertina: progetto grafico Studio Editoriale EDUCatt

Table of contents

III.
Perspectives on resilience

Jihadists' use of cryptocurrencies: undetectable ways to finance terrorism

Daniele Maria Barone

Nota autore

Daniele Maria Barone è laureato in Marketing e Comunicazione presso l'Università IULM di Milano, ha conseguito un master in International Relations presso ASERI Graduate School of Economics and International Relations – Università Cattolica del Sacro Cuore e ha approfondito i suoi studi nel campo della statistica e del marketing con un certificato in Business Analytics alla HBX | Harvard Business School. Si è specializzato in sicurezza nazionale e anti-terrorismo conseguendo l'Executive Certificate in Counter-Terrorism Studies presso l'International Institute for Counter-Terrorism (ICT) di Herzliya, Israele.
Prima di dedicarsi alla ricerca nel settore dell'anti-terrorismo, ha lavorato per diversi anni nel Digital Marketing ricoprendo il ruolo di Project Manager e Marketing Specialist. Data la sua esperienza lavorativa e di studio in ambito comunicazione, economia e anti-terrorismo, i suoi interessi di ricerca sono cyber-jihad, strategie di comunicazione dei gruppi terroristici e metodi di finanziamento al terrorismo.

Abstract

International Islamic terrorist organizations have become fully recognized actors of globalization, whit no borders to group their activities, except through their ideology, rooted in their interpretation of Islam. Their financial resources branch out in the management of physical territories, a global illegal network, organized or small crimes, extortions, donations and they are more and more shifting in the online realm. Indeed, modern financial tools and, in particular, cryptocurrencies, are covering an emerging role in terrorism financing and money laundering. Starting from documented cases of jihadists' use of cryptocurrencies and the most recent developments either in global Islamic terrorism or in modern finance, this paper is aimed at analysing where institutions should intervene in this field and which aspects should be accurately monitored in order to prevent terrorists' illegal use of such an innovative financial resource as cryptocurrencies.

Keywords

Terrorism, jihad, Financing, Cryptocurrency, bitcoin

1. Introduction

In the last year, Daesh lost 98% of its self-proclaimed territories. The majority of its fighters living in its strongholds died during the attacks (70,000 of the estimated 100,000) or became scattered all over the world (approximately 10,000 foreign fighters are thought to have returned to their countries of origin, others have fled into Turkey or have joined affiliates in Egypt, Libya, South-East Asia, Iraq, and Syria). Furthermore, over 130 leaders had been eliminated and millions of people had been liberated.

Even though, as Daesh, the largest part of global and local Islamic terrorism, is facing a decentralized phase, Islamic terrorist groups are still very far from being less cohesive and definitively crushed. Their flexibility and ability to regrow have proven that Islamic terrorist groups are able to use modern technologies at their own advantage to find new ways to spread their ideology, increase the cohesion among their members, weaken and terrorize their enemies, and raise money.

Islamic terrorist organizations have become fully recognized actors of globalization, whit no borders to group their activities, except through their ideology rooted in their interpretation of Islam. Their financial resources work mostly in the same way of their propaganda, branching out in the management of physical territories, a global illegal network, organized or petty crimes, extortions, donations and, more and more, in the exploitation of online modern financial tools: decentralized, up to date, and flexible.

An emerging role in terrorism financing in the online realm is covered by the misuse of cryptocurrencies. Due to a lack of a broadly shared international legal framework to regulate and detect the identity of the people involved in the transactions, cryptocurrencies are becoming progressively broadly used in financial operations related to money laundering, online scams and donation campaigns aimed at financing terrorist groups. Indeed, sporadic evidence of terrorists' use of digital currency has been found since 2012 prevalently among activists at various levels including Daesh or Al-Qaeda, support groups or propaganda, and individuals[1].

Despite the current attention from institutions at both national and international level aimed at countering terrorist groups from exploiting the online realm to raise funds, sometimes the lack of reliable data (due, in a large part, to the anonymity of the users involved in these money transfers) still represents this issue as a grey area that only recently has been discussed as a real threat.

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

Hence it is relevant to understand either the reasons why virtual currencies can be used as an untraceable tool for illegal purposes in general or how terrorists (global Islamic extremist groups in particular) have and will be able to spread their use among their members to get economic support.

This analysis aims at understanding where institutions should intervene and which aspects should be monitored in order to prevent terrorism illegal use of such an innovative financial resource as cryptocurrencies.

2. Modern ways to finance terrorism

Before deepening the analysis on the use of virtual currencies for terrorist purposes, it is useful to give an insight about how, in general, cryptocurrencies work, in order identify which are the weak points that make them such a valuable economic resource for Islamic terrorist organizations.

2.1 How do cryptocurrencies work and how the illegal network evolves around them

Bitcoin is the largest and best-known cryptocurrency. Made up by an anonymous developer who based its functioning on the idea of a virtual currency, not subject to any government or any type of control, spread by the computer engineer Wei Dai in 1998[2]. Other versions of cryptocurrency had been launched but never fully developed when bitcoin became available to the public in 2009. Nowadays different type of cryptocurrency are also available (e.g. Ethereum or Zcash or Litecoin) and all of them, so far, have as a common denominator the possibility to store or process them in a cyber-space characterized by a lack of traceability or control[3].

Cryptocurrencies work in a different way compared to other traditional e-payment networks, as Visa or Paypal, indeed, they are not run by a single company or person[4]. The system develops itself through a network where there is no government, financial institution or any other authority able to have control over it, thus it is completely decentralized. Furthermore, anyone who owns cryptocurrency operates in anonymity: there are no account

[2] W. Dai (1998) *B-Money*. Available at http://www.weidai.com/bmoney.txt

[3] M. Jain (December 14, 2017) *How to use everyday accounting tools to understand cryptocurrency*. HBX Business Blog – Harvard Business School. Available at https://hbx.hbs.edu/blog/post/how-to-apply-everyday-accounting-tools-to-understand-cryptocurrency?utm_source=linkedin&utm_medium=social&utm_campaign=FA

[4] N. Popper (October 1, 2017) *What is Bitcoin and How Does It Work?* The New York Times. Available at https://www.google.it/amp/s/mobile.nytimes.com/2017/10/01/technology/what-is-bitcoin-price.amp.html

numbers, names or any other identifying features that connect the e-value to their owners[5].

E-values overcome the principle of trust on which payment in cash (and world economy) rely upon, by ensuring a system based on an encrypted network of users which establish the reliability of the transactions through a chain of digital signatures[6].

Being a system which runs through a network, there's the necessity to announce all transactions publicly; the public can see that someone is sending an amount of money to someone else, but without information linking the transaction to anyone, same as the level of information released by stock exchanges, where the time and size of individual trades are made public but without telling who the parties are.

The peer-to-peer authentication process is encrypted as senders and receivers are identified only by digital public-key cryptography (i.e. pseudonyms) and every message is signed by its sender and encrypted to its receiver (i.e. private-key cryptography)[7].

It is very easy to open an e-wallet for crypto-values which allows to earn cryptocurrencies by exchanging real money with crypto-values[8], by accepting them as a mean of payment or by "mining" them by solving extremely challenging mathematical problem[9] or use them to purchase goods or ser-

[5] B. Marr (January 17, 2018) *A Complete Guide to Bitcoin in 2018*. Forbes. Available at https://www.forbes.com/sites/bernardmarr/2018/01/17/a-complete-beginners-guide-to-bitcoin-in-2018/#3484762b4418

[6] "Blockchain acts as a public ledger showing all transactions, though the identities of participants are obscured. Each block has a cryptographic link to the previous one. Every addition of a new, linked block to the chain makes it harder for a rogue miner to steal bitcoin by rewriting the sequence of transactions." O. Kharif, M. Leising (January 29, 2018) *Bitcoin and Blockchain*. Bloomberg. Available at https://www.bloomberg.com/quicktake/bitcoins

[7] G.F. (January 27, 2014) Cryptographic Currency – Washing virtual money. The Economist. Available at https://www.economist.com/2014/01/27/washing-virtual-money

[8] "Exchanges such as Coinbase, founded in 2011, offer the easiest way for the general public to buy and sell mainstream cryptocurrencies like bitcoin, Litecoin, and Ethereum. But users have to register with their real identities and prove their cryptocurrency was acquired legally. That makes them less appealing for criminals. Cashing out small amounts of bitcoin is still possible, but it's becoming more difficult to do so without attracting law enforcement attention." D. Gilbert (March 19, 2018) *Criminals are racing to cash out their bitcoin – Here's How They're Doing It*. Vice. Available at https://news.vice.com/en_ca/article/7xdzqa/criminals-are-racing-to-cash-out-their-bitcoin-heres-how-theyre-doing-it

[9] A. Rosic (December 21, 2016) *What is Bitcoin Mining? A Step-by-Step Guide*. Huffington Post. Available at https://www.huffingtonpost.com/ameer-rosic-/what-is-bitcoin-mining-a-_b_13764842.html

vices, allowing transactions of large amount of money within an hour at most[10].

All of these features, adept at providing either anonymity or security to e-value storage or transactions, represent also a risk in order to detect who, where or how much is using cryptocurrency to finance illegal activities. Indeed, even though cryptocurrency represents the next stage of finance, the freedom allowed by the whole system doesn't let enough control over it in order to effectively prosecute organized crime and terrorism financing or detect and prevent it.

Unfortunately, the old rule of "following the money" when trying to track down those who commit crimes in the dark web hasn't proven to be useful so far.

An estimation about how much cryptocurrency is quite entirely shaping around illegal purposes alleges that 44% of all bitcoin transactions are associated with illegal activities (representing around $72 billion per year) such as hacks, money laundering and the trading of drugs and illegal pornography[11]. bitcoin (as other types of cryptocurrency) and illegal activities seem to be so deeply linked to each other that if criminals would stop using it, its value could consequently fall[12], due to the discharging of the most majority of the people who build the network at the base of the cryptocurrency functioning and, therefore, at the base of its increasing value[13].

Since the revolution in the drug selling brought up by the deep web website Silk Road in 2011, which allowed users to buy drugs from an e-commerce directly online, many times shut down but always somehow replaced[14] and still available with detailed instructions about how to reach it from the sur-

[10] Satoshi Nakamoto (pseudonym used by the anonymous bitcoin developer) *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at https://bitcoin.org/bitcoin.pdf

[11] S. Foley, J.R. Karlsen, T.J. Putniņš (January 2018) *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?* University of Sydney – University of Technology Sydney – Stockholm School of Economics in Riga. Available at https://bit.ly/2GtHg5r

[12] A. Sulleyman (January 24, 2018) *Bitcoin price is so high because criminals are using it for illegal trades, research suggests*. The Independent. Available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-fall-criminals-blockchain-anonymous-cryptocurrency-zcash-monero-dash-a8174716.html

[13] M. Del Castillo (December 21, 2017) *Think Tank Links Rising Bitcoin Price to Terrorist Use*. Coindesk. Available at https://www.coindesk.com/u-s-think-tank-finds-rising-bitcoin-price-linked-terrorist-interest/

[14] (July 21, 2017) *Two of the biggest dark-web markets have been shut down – History suggests that other sites will soon fill the void*. The Economist. Available at https://www.economist.com/graphic-detail/2017/07/21/two-of-the-biggest-dark-web-markets-have-been-shut-down

face web[15], many have been the exploitation of the online realm to directly finance illegal activities. As the website AlphaBay, allegedly created in 2014 by Alexandre Cazes, a 26-year-old Canadian living in Thailand, which had almost 250.000 users (among buyers and sellers) with about 369.000 listings for drugs, guns, fake IDs, malware and other illegal goods[16].

This two cases, as many other still present in the dark web, represent a sort of Amazon-like open black markets websites with no regulations, which allow the match of demand and supply in the illegal items field.

Also existing and consolidated transnational crime or terrorist groups are exploiting the cybercrime market and are therefore buying access to technical skills. Indeed, organized crime groups are using centralized virtual currencies like WebMoney and Perfect Money or decentralized cryptocurrencies like bitcoin to better cover their financial footprints.

Latin America and the Caribbean was home to the first major international virtual currency laundering scandal in 2013, with the laundering of $6 billion of illicit transactions tied to drug trafficking, investment fraud, credit card fraud and data theft.

Nowadays drug cartels are employing the so-called "money-mule" networks, which structure virtual and conventional transactions into smaller and more innocuous-looking sums, providing a commission between 3% or 5% per transaction[17].

Some of these online money laundering, developed around transactions of small amount of money, can take place inside the most unsuspecting web platform as, for instance (without the knowledge of their developer) Massive Online Role Playing Games (MMORPG), as Second Life or World of Warcraft, which provide to criminal organizations an undetectable method to launder big amounts of money in the form of cryptocurrencies. The entire process usually works in the following way: open an account on a MMORPG; purchase its virtual currency (usually with a stolen credit card or with cash by purchasing a prepaid card); sell back the virtual currency through the black market community, or to virtual money exchange platform[18].

[15] *Guide On How To Access The Silk Road 3.0 (3.1)*. Available at https://silkroaddrugs.org/guide-on-how-to-access-the-silk-road-3-0/

[16] B. Van Voris, C. Strohm (July 20, 2017) *Criminals' Online Market Targeted by U.S. After Founder Dies*. Bloomberg. Available at https://www.bloomberg.com/news/articles/2017-07-20/u-s-looks-to-seize-assets-tied-to-dark-web-site-alphabay

[17] T.L. Quintero (September 13, 2017) *The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime*. InSight Crime. Available at https://www.insightcrime.org/news/analysis/connected-black-market-how-dark-web-empowered-latam-organized-crime/

[18] J.L. Richet (2013) *Laundering Money Online: a review of cybercriminals' methods*. Tools and Resources for Anti-Corruption Knowledge, United Nations Office on Drugs and Crime

The whole process allows the criminal organization to clean its money and to make very hard to track down every step in order to understand which actors have taken part in the mechanism.

All these examples related to the uses of cryptocurrency in order to finance small criminality or transnational criminal organization are directly linked to Islamic terrorism[19]. As previously explained, terrorism is strictly bond with criminal organizations, which allow terrorist groups to organize terrorist attacks or enlarge their recruitment network (as Daesh did in Trinidad and Tobago or in Latin America[20]) also in territories where they don't have a strong physical presence and, concerning the fundraising purposes, they provide a financial resource linked to their criminal activities (e.g. drug trafficking, kidnapping, smuggling).

Dark Web and cryptocurrencies represent of course an innovative instrument for either finance or freedom of speech but is also evolving and consolidating as a neutral territory, with no regulation, which surely has the characteristics of a profitable arena for terrorist groups. In fact, the most modern types of cryptocurrencies, as Zcasch, are developing in order to allow secure transactions using a different method that may become able to allow offline transactions that don't rely on the physical transfer of an e-wallet[21]. This will make the use of these currencies viable in parts of the world without reliable internet access and increase the undetectable feature of e-values.

The interest of global Islamic terrorist groups as Daesh in the cryptocurrencies field is not at its early stages; they began to analyze and encourage their use since the first introduction of this modern financial tool in the market. Hence, even though the use of crypto-values still doesn't represent their primary financial resource, they have proven of being able to exploit them in the best possible way in terms of use of their lack of traceability. Understand now how they're using this still unknown field, could be crucial to prevent an important source of strength they could be able to consolidate in the near future. Moreover, the lesson learned by lone wolves attacks has taught us that hybrid terrorism is a low-cost invest, thus the most urgent issue

(UNODC). Available at http://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf

[19] M. Bihter (2011) *Money Laundering And Terrorism As A Global Threat And A Comparison Between United States And Turkey*. Ankara Bar Review. Available at http://www.ankarabarosu.org.tr/siteler/AnkaraBarReview/tekmakale/2011-2/6.pdf

[20] T.L. Quintero (September 13, 2017) *The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime*. InSight Crime. Available at https://www.insightcrime.org/news/analysis/connected-black-market-how-dark-web-empowered-latam-organized-crime/

[21] 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

is related to stopping terrorist groups from establishing a transnational network able to transfer from the largest to the smallest amount of money.

2.2 Daesh and cryptocurrencies: cases from early stages till the most recent uses

The analysis of this paragraph will focus on the main cases which prove the increasing interest of Islamic terrorist organizations towards the use of digital currencies, in a chronological order. This will highlight the growing amount of money and the more and more imaginative methods that Islamic terrorist groups are using in order to be less detectable and bring more followers who actively provide economic strength to their cause.

– ***Hawala***: prior to the invention of cryptocurrencies, for the past couple of decades, foreign donations to terrorist organizations have been delivered by another method used to transfer money anonymously, which is still active today: the *hawala*[22] network[23]. The *hawala* system, a sort of extremely fast (1 or 2 days at most) and very cheap (5% at transaction is the only cost required) remittance system network, generally used by migrant workers who frequently send money to relatives and friends in their countries of origin, is able to provide anonymity for cash transfers and donations[24]. Hawala is a decentralized network which allows individuals or groups, who want to donate money to a terrorist organization, to pass money through an *hawaladar* in their country, to another *hawaladar* in the destination country who delivers the money to the addressee, allowing terrorist groups to transfer their own funds or resources from one location to another. The whole system created many layers of intermediaries so that donors and ultimate recipients may not be known to one other.
  Cryptocurrencies, bitcoin as first, made anonymous transactions faster and more secure, overlapping the need of basing the whole operation on people's trust.
– "**Fund the Islamic Struggle Without Leaving a Trace**": the first known case of exploitation of cryptocurrency for Islamic terrorism purposes was

[22] *"Transfer or Remittance"* in Arabic. "A system of money transfer based on promises and honor, practiced in the Middle East and parts of Asia and Africa". Collins English Dictionary – Complete and Unabridged, 12th Edition 2014 © HarperCollins Publishers.

[23] M. Zencho (August 17, 2017) *Bitcoin for Bombs*. Council on Foreign Relations. Available at https://www.cfr.org/blog/bitcoin-bombs

[24] P.M. Jost, H.S. Sandhu (January 2000) *The* hawala *alternative remittance system and its role in money laundering*. United States Department of the Treasury Financial Crimes Enforcement Network (FinCEN) in cooperation with INTERPOL/FOPAC. Available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-Hawala-rpt.pdf

allegedly registered in 2012, when an anonymous website was uploaded in the deep web for the purpose of raising money anonymously through *sadaqah*[25] to support the Islamic fight against the United States, by using bitcoins. Even if it is not sure that the website presented by the explanatory title "Fund the Islamic Struggle Without Leaving a Trace[26]" was made by a terrorist group's affiliated or was only a scam, it has been registered that it had received an amount of 5 bitcoins when the bitcoin exchange rate was more or less $10[27].

– **Ghost Security Group investigations**: not verified reports made by the hacker group "Ghost Security Group" following IS terrorist attack at Bataclan in November 2015 showed that, since 2012, other bitcoins addresses in the dark web where found being connected to Daesh[28]. In one of these accounts one where found having the equivalent of almost $3 million which, according to the hacker group, were earned mostly by donations[29].
– **Golden coins from occupied territories**: digital currencies have not being used only for donations to the terrorist organization through the dark web, but also to sell items. A topic example is related to the deep web website, also advertised on Dabiq, which appeared for the first time in 2014, to sell the golden, silver, and copper coins used in the areas under IS control in Iraq and Syria as means of payment[30]. The coins minted by the Islamic State apparently became superfluous when Daesh was driven out of the self-proclaimed caliphate territories. Thus, now that these coins are no longer in use, the group is attempting to sell them as souvenirs[31].

[25] An Islamic term for "voluntary charity". Collins Dictionary.

[26] Krypt3ia (October 14, 2013) *Darknet Jihad*. Available at https://krypt3ia.wordpress.com/2013/10/14/darknet-jihad/

[27] ICT Cyber-Desk Periodic Review (October-November 2013) *Cyber-Terrorism Activities Report No. 6*. IDC Herzliya – International Institute for Counter-Terrorism (ICT). Available at https://www.ict.org.il/UserFiles/Cyber%20Report%206.pdf

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

[29] J. Sagar (November 14, 2015) *Bitcoin 3 Million Dollars*. News BTC. Available at https://www.newsbtc.com/2015/11/14/isil-militants-linked-to-france-terrorist-attacks-had-a-bitcoin-address-with-3-million-dollars/

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

[31] The Meir Amit Intelligence and Terrorism Information Center (2018) *In view of its financial problems, ISIS is selling coins that it minted at the time of the Islamic State. Payment for the coins is made via an international clearing system*. Available at http://www.terrorism-info.org.il/app/uploads/2018/01/E_003_18.pdf

– ***Bitcoin wa Sadaqat al-Jihad***: in the summer of 2014, an article titled *Bitcoin wa Sadaqat al-Jihad* ("Bitcoin and the Charity of Jihad") was published in an online blog. The article explained the various strategic and religious reasons for jihadists to use bitcoin. It promoted the use of bitcoin virtual currency as a means of limiting economic support for infidels and circumventing the Western banking system. It also recommended to use bitcoin for ideological-religious reasons as well as for its technological characteristics, and insisted on the advantages of the system that enables the issuing of this currency." It also stressed that the advantages of using bitcoin include: "prevention of counterfeiting; it is anonymous and untraceable; it is not subject to legislation; and it has global distribution[32]."
– ***Jahezona***: the first reliable case of fundraising by using crypto-values, directly connected to a terrorist organization, began in July 2015 when the *Ibn Taymiyya Media Center* (ITMC), the media wing of the Mujahideen Shura Council in the Environs of Jerusalem (MSC), a collection of Salafi-jihadist groups in Gaza, run a social media fundraising campaign: *Jahezona*[33]. The fundraising campaign was arguing that such donations fulfilled a religious obligation to fight for Islam. The campaign regularly posted graphics showing the group's desired weapons and ammunition and their respective costs. In late June 2016, the campaign added the option to pay in bitcoin, posting infographics on Twitter with QR codes linking to a bitcoin address. The campaign received two transactions which raised a total amount of 0.929 BTC (approximately $540) and on August 20, the funds were transferred to other addresses whose ownership is unknown. Then it is possible that the campaign's organizers made these transactions by themselves in order to test the bitcoin address.

  It results interesting that one chain of transactions tracked from the *Jahezona* address also deposited bitcoin funds into addresses owned by other bitcoin sites, like "matbea.com" or "cloudbet.com" or "localbitcoins.com", mostly used to sell bitcoins in person and popular resources for people seeking anonymity to cash out bitcoins as a sort of exchange withdrawal service[34].

  The *Jahezona* campaign is still active. In 2018 on the *Jahezona* Telegram group has been identified a new bitcoin address, which revealed a series of 15 transactions from July 1, 2016 to January 12, 2018, many of

[32] *Bitcoin wa Sadaqat al-Jihad*. Available at https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf

[33] "Equipe us" in Arabic.

[34] Y. Fanusie (August 24, 2016) *The New Frontier in Terror Fundraising: Bitcoin*. The Cipher Brief. Available at https://www.thecipherbrief.com/column/private-sector/the-new-frontier-in-terror-fundraising-bitcoin

which are valued at tens or hundreds of dollars, with a few transactions amounting to thousands of dollars, reaching picks of large sums equivalent to $289,273.87 and $123,020.68[35].

– The case of a computer intruder with ties to I***slamic State Hacking Division***, one of Daesh's cyber unit, **Ardit Ferizi**: an ethnic Albanian who was raised in Kosovo, also known by the username "**Albanian hacker**", who in August 2015 demanded payment of two bitcoins (approximately $500 at the time) from an Illinois Internet retailer, in exchange for removing bugs from its computers[36]. Using the data extracted from the retailer's server, the Albanian hacker put together a "kill list" for IS with identities of 1.351 US government and military personnel[37].
– ***Akhbar al-Muslimin*** **fundraising campaign**: in November 2017, one month after the fall of Raqqa, a banner for donations of bitcoins was launched on the IS-affiliated website which publishes news from the Islamic State, *Akhbar al-Muslimin*. The website has posted a link for bitcoin donations claiming "Click here to donate bitcoins to the (*Akhbar al-Muslimin*) website – do not donate from *zakāt*[38] funds"(as shown in the orange banner of the image below). The donations are presented as a support for the website, but may probably have been used by Daesh to restore its propaganda machine or fund terrorist attacks abroad[39]. Further assessments have detected that the link no longer directs to CoinGate, showing how quickly Daesh's online branches adapt to avoid being tracked[40].
– **Bahrun Naim**: the alleged planner of the 2016 attacks in Jakarta that killed eight people including four militants, who in 2017 was reported to

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

[36] T. Johnson (July 20, 2016) *Computer hack helped feed an Islamic State death list*. Mc Clatchy DC Bureau. Available at http://www.mcclatchydc.com/news/nation-world/national/article90782637.html

[37] Z.K. Goldman, E. Maruyama, E. Rosenberg, E. Saravalle, J. Solomon-Strauss (May 2017) *Terrorist use of virtual currencies: containing the potential threat*. Center for a New American Security (CNAS). Available at https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-TerroristFinancing-Final.pdf

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

[39] The Meir Amit Intelligence and Terrorism Information Center (December 06, 2017) *Drive for bitcoin donations on an ISIS-affiliated website*. Available at http://www.terrorism-info.org.il/en/drive-bitcoin-donations-isis-affiliated-website/

[40] Y.J. Bob (January 28, 2018) *ISIS, other jihadists increase bitcoin use after fall of Caliphate*. The Jerusalem Post. Available at https://www.jpost.com/Middle-East/ISIS-Threat/ISIS-other-jihadists-increase-bitcoin-use-after-fall-of-Caliphate-540079

have used bitcoin to transfer money to the **wife of Arif Hidayatullah** (a militant who was arrested by Indonesian counter-terrorism police unit) and to send money to militants and fund terrorist activities[41].

– ***Al Sadaqah* donation campaign**: in November 2017 the *Al-Sadaqah* organization, presenting itself as a charity organization, began a still ongoing fundraising campaign on Telegram and other social media such as Twitter (see the image below[42]) to raise money, in bitcoin[43], from Western supporters, to finance the *mujahideen* fighting against the Assad regime in northeastern Syria. The campaign has been circulated on channels identified as close to *Hay'at Tahrir Al-Sham* (HTS), Al-Qaeda, and the global jihad in general[44]. The fundraising campaign opens with a quote by 12th-century Islamic scholar *Ibn Taymiyyah*: "Whoever is unable to take part in jihad physically but is able to take part in jihad by means of his wealth is obliged to take part in jihad by means of his wealth. So those who are well off must spend for the sake of Allah."
  Since then, *Al Sadaqah* has broadened its appeal, starting to solicit funds through additional cryptocurrencies, as Zcasch, that offer even more privacy than bitcoin[45].
– **Zoobia Shahnaz**: a 27-year-old lab technician, US citizen born in Pakistan, arrested in December 2017 while trying to fly from the United States to Istanbul and from Turkey to Syria[46]. After allegedly being radicalized online since 2015 and have been in contact with IS members while volunteering for the *Syrian American Medical Society in Jordan* in the *Zataari* refugee camp, in the city of Amman in 2016, she came back in the US and provided fake information to obtain bank loans and over a dozen credit cards in order to transfer the money into bitcoin and other cryp-

[41] I.L. Tisnadibrata (September 01, 2017) *Indonesia Tracks Online Funding of Terror Groups*. Benar News. Available at https://www.benarnews.org/english/news/indonesian/online-payments-01092017155456.html

[42] Al Sadaqah Twitter page. Available at https://twitter.com/alsadaqah1

[43] M. Del Castillo (December 21, 2017) *Think Tank Links Rising Bitcoin Price to Terrorist Use*. Coindesk. Available at https://www.coindesk.com/u-s-think-tank-finds-rising-bitcoin-price-linked-terrorist-interest/

[44] MEMRI Cyber & Jihad Lab (November 13, 2017) *Online Campaign In English Raising Funds For The Jihad In Syria In Bitcoin*. MEMRI. Available at http://cjlab.memri.org/latest-reports/online-campaign-in-english-raising-funds-for-the-jihad-in-syria-in-bitcoin/

[45] B. Forrest, J. Scheck (February 20, 2018) *Jihadists See a Funding Boon in Bitcoin*. The Wall Street Journal. Available at https://www.wsj.com/articles/jihadists-see-a-funding-boon-in-bitcoin-1519131601

[46] The Meir Amit Intelligence and Terrorism Information Center (December 14-20, 2017) *Spotlight on global jihad*. Available at http://www.terrorism-info.org.il/en/spotlight-global-jihad-december-14-20-2017/

tocurrencies to IS[47]. As prosecutors alleged, between March and August 2017 she scammed various financial institutions out of roughly $85,000, then purchased approximately $62,000 worth of bitcoin and other cryptocurrencies subsequently transferred to shell entities in Pakistan, China, and Turkey to benefit the terrorist group while "concealing the identity, source, and destination of the illicitly obtained monies[48]".

– **Telegram Open Network (TON)**: pointing out the lack of a mass-market cryptocurrency which can be used for daily transactions, the lack of consumer activity and the need for technical know-how when interacting with existing digital currencies[49], the team of Telegram announced in December 2017, that within 2018 will develop and make available a faster, with more advanced capabilities and user-friendly new type of crypto-value called Gram[50]. Since 2015, when it was used in the planning of the Paris attacks, Telegram has emerged as jihadis' preferred app for encrypted communications, including planning or to claim responsibility for its attacks[51]. Indeed, Telegram founder and CEO, Mr Durov, in 2016, has been officially asked by the Congress of the United States, after noting that hundreds of channels affiliated with Daesh and other terrorist organizations still find refuge in Telegram's encrypted service, to do all in his power to prevent terrorists from exploiting Telegram to advance their lethal cause[52]. Even though the right path to follow in the policies filed shouldn't accept

[47] H. Alexander (December 14, 2017) *New York woman charged with sending $85,000 in bitcoin to support Isil*. The Telegraph. Available at https://www.telegraph.co.uk/news/2017/12/14/new-york-woman-charged-sending-85000-bitcoin-support-isil/

[48] Department of Justice – U.S. Attorney's Office – Eastern District of New York (December 14, 2017) *Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists. Defendant Stole and Laundered Over $85,000 Using Bitcoin and Other Cryptocurrencies*. Available at https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists

[49] H. Nasser (January 09, 2018) *Exclusive: Telegram ICO (TON) Leaked Whitepaper Reveals Ambitious Plans*. CryptoVest. Available at https://cryptovest.com/news/exclusive-telegram-ico-ton-leaked-whitepaper-reveals-ambitious-plans/

[50] DeCenter YouTube Channel (December 22, 2017) *Telegram Open Network – TON (Promo Final Version)*. Available at https://www.youtube.com/watch?v=3O-jnS72gY4

[51] J. Warrick (December 23, 2016) *The 'app of choice' for jihadists: ISIS seizes on Internet tool to promote terror*. The Washington Post. Available at https://www.washingtonpost.com/world/national-security/the-app-of-choice-for-jihadists-isis-seizes-on-internet-tool-to-promote-terror/2016/12/23/a8c348c0-c861-11e6-85b5-76616a33048d_story.html?utm_term=.0a8b5bf40b52

[52] S. Stalinsky (March 30, 2018) *The Imminent Release Of Telegram's Cryptocurrency, ISIS's Encryption App Of Choice – An International Security Catastrophe In The Making*. MEMRI. Available at https://www.memri.org/reports/imminent-release-telegrams-cryptocurrency-isiss-encryption-app-choice-%E2%80%93-international

to stop progress in order to avoid terrorist undetectable activities, given the previous analysis about the exploitation of the encrypted chat services and the technical skills that jihadists have proven to have in using dark web and cryptocurrencies at their own advantage, it comes quite clear that such a user-friendly blockchain technology, as the one proposed by Gram, would put another potentially very powerful tool in the terrorists' hands. If it will still not be clear which are going to be the precise measures to avoid terrorist exploitation provided by TON blockchain, then it will be impossible to foresight how many and how dangerous will be terrorism methods to exploit this new encrypted tool.

– **Bitcoin to fund jihadi training camps**: an IS terrorist, known only as Mohammed G, plundered the bank accounts of murdered holiday-makers Rod Saunders, 74, and his wife Rachel, 63. The couple was abducted by four terrorist group's affiliated in the Ngoye Forest Reserve, just 80 miles north of Durban, South Africa, on February 10, 2018. Mohammed G had contact with one of the kidnappers and was ordered to loot and launder their assets. He used their stolen credit card details to buy bitcoin online, which he then spent on Kalashnikov rifles, crossbows and swords. He also worked as an "IS travel agent" who would arrange trips for himself and other people to join Daesh forces in Iraq and Syria. He was arrested in March 2018 when anti-terror cops raided his house in the Southern Dutch city of Maastricht[53].

These cases show that the exploitation of cryptocurrencies by terrorist supporters present some aspects as a **common denominator**:

1. **A global and decentralized network**: Islamic terrorist organizations have become fully recognized actors of globalization, making hard to draw borders to group their activities, except through their ideology rooted in the Islamic extremism. The same happens with their financial resources, which branch out in a global network through the disuse of modern means of communication, cooperation with criminal organizations, and donations or, even more nowadays with Daesh's fragmentation after being forced out of its strongholds and the subsequent reinforcement of the Virtual Caliphate, in the online realm[54].

[53] J. Dirnhuber (August 29, 2018) *Funding Hate ISIS fanatics plundered bank accounts of Brit couple murdered by jihadis in South Africa and used money to buy bitcoin and fund jihadi training camp*. The Sun. Available at https://www.thesun.co.uk/news/7122832/rod-saunders-rachel-isis-bank-accounts-terror-south-africa/

[54] E. Azani (March 06, 2018) *Global Jihad – The Shift from Hierarchal Terrorist Organizations to Decentralized Systems*. International Counter Terrorism Institute – Herzliya. Available at https://www.ict.org.il/Article/2210/Global_Jihad_Shift_from_Hierarchal_Terrorist_Organizations#gsc.tab=0

2. **The threat behind an improved online radicalization process**: usually requests for donations to terrorist groups are explained to their supporters by the principles of ***zakāt***[55] or ***sadaqah***[56] in order to justify their actions by exploiting the *Sharia* law. This aspect highlights that in the most majority of the cases sympathizers or followers of Islamic extremist ideologies are usually brought closer and closer to finance terrorist organizations by passing through a well-structured radicalization process. Furthermore, nowadays radicalization is a process that can also take place entirely online[57], suggesting that the group will push more and more efforts in order to optimize effective methods to get economic support from small or wealthy donors or to launder money raised from illegal activities, by exploiting the spread of their extremist religious ideologies through the web-space[58].
3. **Modern terrorism is a low-cost investment**: in a 2007 video, Mustafa Abu al-Yazid, Al Qaeda's finance chief, claimed: "there are hundreds wishing to carry out martyrdom-seeking operations, but they can't find the funds to equip themselves."[59]. Since a few years ago terrorist attacks don't cost anymore a prohibitive amount of money as used to be for Al-Quaeda in the 2000s given that they don't require anymore the use of complex operative or tactical planning. In fact, the lesson learned by lone wolves attacks has taught that a terrorist attack in the hybrid warfare is a low-cost investment: they can be carried out by one individual with rudimental tactical knowledge and no operative skills, using extremely cheap weapons as knives or amateur bombs. Thus the most urgent issue is related to stopping terrorist groups from establishing a transnational network able to transfer from the larger to the smallest amount of money. This approach would either cut decisively terrorists' financial resources or prevent them from easily planning a large number of terrorist attacks around the globe.

[55] 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 word *zakāt* origins comes from Persian and Kurdu languages, meaning "almsgiving".
[56] An Islamic term for "voluntary charity".
[57] I. von Behr, A. Reding, C. Edwards, L. Gribbon (2013) *Radicalisation in the digital era. The use of the internet in 15 cases of terrorism and extremism*. RAND Europe. Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf
[58] Il Sole 24 Ore (May 10, 2018) *Money transfer illegali per finanziare la Jihad: arrestati 14 fiancheggiatori*. Available at http://www.ilsole24ore.com/art/notizie/2018-05-10/terrorismo-arrestati-14-fiancheggiatori-formazioni-jihadiste-081156.shtml?uuid=AEGPd1lE
[59] E. Serravalle, E. Rosenberg (January 09, 2018) *Bitcoin can help terrorists secretly fund their deadly attacks*. FoxNews. Available at http://www.foxnews.com/opinion/2018/01/09/bitcoin-can-help-terrorists-secretly-fund-their-deadly-attacks.html

3. Anti-money laundering and counter-terrorism financing: current governmental and religious approaches to tackle the issue

As pointed out during the International Conference on terrorism financing "**No Money for Terror**" held in Paris the 25-26th of April 2018, which has gathered Ministers from 80 countries and nearly 500 experts, a growing number of States is criminalizing terrorism financing as a standalone offense but the number of terrorism-financing cases being successfully prosecuted by UN Member States' judicial systems is still limited, due to the difficulty of proving the intent that the funds would be used for terrorism purposes[60].

Undoubtedly, the most undetectable types of terrorism funding are related to the illegal use of crypto-values, which allow the perpetration of untraceable donations or money laundering to finance terrorist organizations.

As virtual currencies become more widely accepted and play an expanding role in trading, governments have increasingly come to recognize that they are a potentially enduring reality, which still needs to be properly regulated in order to prevent its illegal use.

The following decisions or regulations at either governmental or religious level, highlight the most recent developments regarding counter-terrorism financing by cryptocurrencies:

– **United States – Financial Technology Task Force**: in January 2018 US lawmakers introduced a bill aimed to form a new task force. Its purpose would be to provide rewards for information leading to convictions related to the terrorist use of digital currencies and to encourage the development of tools and programs to combat terrorism and illicit use of digital currencies[61]. The task force would primarily focus on researching ways that terrorism can be financed through cryptocurrencies and subsequently propose regulations to counter these illegal activities[62].
– **Australia – Anti-Money Laundering And Counter Terrorism Financing Act (AML/CTF)**: in April 2018 AUSTRAC (Australia's financial

[60] Security Council Counter-Terrorism Committee (April, 30 2018) *CTED Executive Director participates in international conference on terrorism financing*. Available at https://www.un.org/sc/ctc/news/2018/04/30/cted-executive-director-participates-international-conference-terrorism-financing/

[61] Financial Technology Innovation and Defense Act 115th Congress – 2d Session (January 10, 2018) Available at https://www.congress.gov/bill/115th-congress/house-bill/4752/text?q=%7B%22search%22%3A%5B%22congressId%3A115+AND+billStatus%3A%5C%22Introduced%5C%22%22%5D%7D&r=66

[62] W. Zhao (January 17, 2018) *Proposed US Task Force Would Tackle Crypto Use in Terrorism Financing*. CoinDesk. Available at https://www.coindesk.com/proposed-us-task-force-would-tackle-crypto-use-in-terrorism-financing/

intelligence agency) implemented new AML/CTF laws to cover, for the first time, regulation of service providers of cryptocurrencies, including bitcoin. The new laws will strengthen the agency's compliance and intelligence capabilities to help implement systems and controls aimed at minimizing the risk of money laundering, terrorism financing, and cybercrime[63].

– **South Korea and Korea Financial Intelligence Unit (KFIU)**[64]: the new South Korean cryptocurrency account system has entered into force nationwide on January 29, 2018, ending the practice that allowed anonymous trading of cryptocurrencies, by converting existing virtual cryptocurrency accounts to real-name accounts[65]. Moreover, during the Policy Advisory Council meeting held on June 8, the head of KFIU, Kim Geun-ik, spoke about existing money laundering and terrorist financing prevention regulations and proposed to regulate crypto exchanges in the same way the governments does with banks. The KFIU, following leading economies such as the US or Japan, will implement stricter rules for independent financial service providers to prevent money laundering and terrorist financing with rigorous verification processes for large transactions and monitoring of users[66].
– **Estonia**: as other small and fast-moving European countries (e.g. Malta) that in recent times are attracting cryptocurrencies businesses, the Estonian government has recently allowed CoinMetro[67] (a company operating in virtual currencies market) to secure two licenses for cryptocurrency trading activities: "Wallet license" to store cryptocurrencies and "Exchange license" to trade cryptocurrencies for other assets or other types of digital currencies[68]. This initiative has the purpose to create a virtual safe space for businesses with cryptocurrencies that will help to provide a framework

[63] Australian Government – AUSTRAC (April 11, 2018) *New Australian laws to regulate cryptocurrency providers*. Available at http://www.austrac.gov.au/media/media-releases/new-australian-laws-regulate-cryptocurrency-providers

[64] Available at http://www.kofiu.go.kr/eng/sub1/1.jsp

[65] K. Helms (January 30,2018) *South Korea Ends Anonymous Cryptocurrency Trading Today*. bitcoin.com. Available at https://news.bitcoin.com/south-korea-ends-anonymous-cryptocurrency-trading/

[66] (June 12, 2018) *South Korea to Impose Stricter Regulation of Cryptocurrency Exchanges*. Sputnik. Available at https://sputniknews.com/science/201806121065344133-south-korea-regulation-crypto-exchanges/

[67] Available at https://coinmetro.com/about

[68] A. Mizrahi (June 07, 2018) *Estonia Grants Licenses for Wallet and Exchange Services to Coinmetro*. bitcoin.com. Available at https://news.bitcoin.com/estonia-grants-licenses-for-wallet-and-exchange-services-to-coin-metro/

for establishing robust checks for anti-money laundering, counter-terrorism financing, and more detailed customer information.

– **Financial Crime Task Force (FATF)**: the FATF is an intergovernmental organization based in Paris, which currently comprises 35 member States and two regional organizations, has the duty to develop policies to combat financial crimes. The organization published non-binding guidelines in June 2015 to promote a risk-based approach to cryptocurrencies, giving advice about exchanges to be registered or licensed, to verify customers' identities to prevent money laundering, and for suspicious trading to be reported[69]. At the FATF meeting in Paris, held between February 18-23 2018, member countries asked to improve the understanding of money laundering risks relating to cryptocurrencies. Furthermore, even though it is not yet officially confirmed, following the member countries requests, within June 2018 the FATF will start a discussion aimed at introducing binding rules to govern cryptocurrency exchanges. In particular, the next step will take into account whether the 2015 rules are still appropriate and how to work with countries that have moved to ban cryptocurrency trading.
– **Muslim communities on the illegal use of cryptocurrency: a counter-narrative to terrorism propaganda**: while there are attempts to make cryptocurrencies more *Shariah* compliant, it is still not widely clear whether they are permissible in accordance to the *Shariah* law. The clearer answer to this debate came from the *Mufti* Shauqui Alam, the most influential religious authority of Egypt, in January 2018[70]. Even though in Egypt the use of cryptocurrencies is not forbidden, recognizing their illicit use perpetrated by terrorist groups, the *Mufti* issued a *fatwa*[71] prohibiting the use of bitcoins. Shauqui Alam motivated his decision on the ground that exists a similarity between cryptocurrencies and gambling (strictly forbidden by the Quran) due to their price volatility[72].

[69] FATF/OECD (June 2015) *Guidance for a risk-based approach virtual currencies*. Available at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

[70] A. Helmi, B. M. Hasbi, R. Mahzam (April 2018) *Cryptocurrencies: Potential For Terror Financing?* S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Available at https://www.rsis.edu.sg/rsis-publication/icpvtr/co18075-cryptocurrencies-potential-for-terror-financing/#.WyNd_RIzaqQ

[71] A religious edict in the Islamic faith.

[72] M. Sabella (January 01, 2018) *Bitcoin, il* Mufti *del Cairo lancia una* fatwa *contro la criptovaluta*. Corriere della Sera. Available at https://www.corriere.it/economia/18_gennaio_01/bitcoin-mufti-cairo-lancia-fatwa-contro-criptovaluta-a7c062d0-ef18-11e7-97e1-31c2bf5f7cef.shtml

In the case of the *Mufti* Shauqui Alam, the Muslim community developed a counter-narrative to Islamic extremism, able to dismantle its ideology and explain an alternative religious path to the Islamic community which, if strengthened, would be a valuable resource to cut terrorists financial resources through donations.

4. Crime-terror nexus and potential jihadist's uses of cryptocurrencies

The analysis commissioned by the European Parliament TERR Committee[73] about terrorism financing by virtual currencies, published on May 2018, "**Virtual currencies and terrorist financing: assessing the risks and evaluating responses**[74]", has depicted the complex nature of the actors generally involved in extremist groups' online financing. The study gathers the subjects involved in this cyber-threat into distinct groups (lone actors, small-cells, command and control organizations, territory controlling groups) associating them with different funding methods (raising funds, moving funds, storing) that are helpful to identify the actors taking part in the terrorist illegal use of cryptocurrencies and what would be their main purposes in this field.

Hence, in order to try to prevent the next steps in online Islamic terrorist financing field, it is crucial to analyze this phenomenon through a perspective based on a **crime-terror nexus**[75], by comparing criminals' use of digital currencies (that, since now, are far more documented) with the last development of global terrorism. This approach can help to provide a picture of where the real threat of terrorism online financing lies.

4.1 Global terrorist organizations and their support groups

Terrorist organizations which are usually relying on the occupation of territories (as **Daesh** in Iraq and Syria or **al-Shabaab** in Somalia), those without a single established base (as **al-Qaeda**) and their support groups (e.g. **Haq**

[73] European Parliament Committees – Terrorism. Available at http://www.europarl.europa.eu/committees/en/terr/home.html

[74] T. Keatinge, D. Carlisle, F. Keen (May 2018) *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs. Available at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

[75] R. Basra, P.R. Neumann, C. Brunner (2016) *Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus*. The International Center for Studies on Radicalization and Political Studies. Available at http://icsr.info/wp-content/uploads/2016/10/Criminal-Pasts-Terrorist-Futures.pdf

Web site, **Akhbar al-Mulsilimin website**, **Jahezona group**) have already started to exploit the potential of modern financial tools. Despite, in most cases, could be important to study separately the peculiarity and rationale of each global Islamic terrorist group (as much as possible in the complex nature of Islamic extremism), the fact that terrorist exploitation of cryptocurrencies is still at an early stage, allows to find common trends even among totally different extremist Islamic groups which could develop in the following areas:

– **Purchase or sale of illegal items on the dark web**[76]: a large part of global Islamic terrorist groups online activities are still detectable on the surface web but most of it, especially which of those concern operative instructions or one-to-one communications, have been shifted on dark web websites[77] or encrypted end-to-end chat groups (e.g. WhatsApp or Telegram[78]). Besides the radicalization and propaganda purposes, the dark web also represents a sort of Amazon-like open black markets with no regulations, which allows the match of demand and supply of illegal items (e.g. drugs or weapons), where crypto-values have become the prominent mean of payment[79]. Even though there is not yet documented evidence of terrorists massive use of the dark web illegal markets, cases as the drug selling dark website "**Silk Road**" or the recently dismantled **criminal network** operating in Spain, which was producing and distributing synthetic drugs worldwide on the dark web by accepting payments in cryptocurrencies[80],

[76] The deep web (Academic databases, Medical and financial records, subscription only content, organization-specific content) and the Dark web (TOR, illegal activities) make up over 99.8% of the entire web and only less than 0.2% of the web is visible (i.e. surface or public web). It is in this untraceable places of the online network, built around hidden browsers, where the most majority of illegal online activities are perpetrated. Dark web is built around web browsers, the most frequently used are TOR or OPERA, which were meant to protect the anonymity of vulnerable people online. These type of browsers operate in the same way of Google Chrome or Internet Explorer but are able to encapsulate communications in layers of encryption that mask the identity of who is browsing and what they're looking at.

[77] G. Weimann (November 3, 2016) *Terrorist Migration to the Dark Web*. Univeriteit Leiden – The Netherlands. Available at http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html

[78] C. McCoogan (February 2, 2016) *Dark web browser Tor is overwhelmingly used for crime, says study*. The Telegraph – Technology Intelligence. Available at https://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/

[79] (July 21, 2017) *Two of the biggest dark-web markets have been shut down – History suggests that other sites will soon fill the void*. The Economist. Available at https://www.economist.com/graphic-detail/2017/07/21/two-of-the-biggest-dark-web-markets-have-been-shut-down

[80] EUROPOL Press Release (June 28, 2018) *Police seize more than EUR 4.5 million in cryptocurrencies in Europe's bigger ever LSD bust*. Available at https://www.europol.europa.eu/newsroom/news/police-seize-more-eur-45-million-in-cryptocurrencies-in-europe%E2%80%99s-biggest-ever-lsd-bust

suggest that this trend has the potential to become a growing threat which should be carefully monitored. Furthermore, the increasing bond between Islamic terrorists and criminals[81], rooted either in the fact that terrorist organizations are inciting their supporters to commit criminal activities by encouraging them to use funds raised through criminality as a legitimate way of financing the *jihad*[82] or in their cooperation with international crime organizations from low-scale criminality (e.g. sale of counterfeited clothes or electronic devices[83]) to organized crime (e.g. trafficking in drugs, weapons, cultural artifacts[84]), shows a potential growing threat of terrorists' use of dark web black-markets. Moreover, the new terrorist youngest recruits, which are computer literate, will inevitably grow Islamic extremism crime rate on the online realm and, as a consequence, could push more and more in order to increase the exploitation of cryptocurrencies and the dark web to raise funds[85].

– **Receive donations to store or invest money**: global Islamic terrorist organizations have always been relying on large or small, anonymous public donations coming from West-based individuals, members of the diaspora community[86], wealthy supporters (often from Gulf state countries) or like-minded terrorist groups (as in 2012, the Nigerian group Boko Haram reportedly received $250,000 from al-Qaeda[87]), to get financial support. Thus, as already seen in the cases of the donations request by bitcoins on the Al-Qaeda affiliated, Syrian-jihadi group, ***Al-Sadaqah*** **donation**

[81] N. Malik (May 2018) *Terror In the Dark*. Centre of the Response to Radicalization and Extremism. Available at http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

[82] R. Basra, P.R. Neumann, C. Brunner (2016) *Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus*. The International Center for Studies on Radicalization and Political Studies. Available at http://icsr.info/wp-content/uploads/2016/10/Criminal-Pasts-Terrorist-Futures.pdf

[83] E. Kaplan (April, 4 2006) *Tracking Down Terrorist Financing. Council on Foreign Relations*. Available at https://www.cfr.org/backgrounder/tracking-down-terrorist-financing

[84] Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – *Financing of terrorism*. Council of Europe. Available at https://www.coe.int/en/web/moneyval/implementation/financing-terrorism

[85] TE SAT European Union (2017) *Terrorism Situation and Trend Report 2017*. Available at https://www.europol.europa.eu/tesat/2017/

[86] L. Dearden (July 12, 2017) *UK residents donate thousands of pounds a year to Islamist extremist organisations, Home Office reveals*. Independent. Available at https://www.independent.co.uk/news/uk/home-news/british-people-islamist-funding-extremist-organisations-home-office-amber-rudd-uk-isis-terrorism-a7837451.html

[87] T. Keatinge (December 12, 2014) *Finances of jihad: How extremist groups raise money*. BBC News. Available at http://www.bbc.com/news/world-middle-east-30393832

campaign[88] or with the media group associated with Daesh, "**Technical Support of Afaq Electronic Foundation**", which offered an alternative to secure online purchasing via the Zcash virtual currency[89], global Islamic terrorist organizations are already inciting their followers, scattered across the globe, to give economic support (warping the Islamic principles of *zakāt*[90] or *sadaqha*[91]) through the online realm. The money collected by these donation campaigns, as in the case of the ***Akhbar al-Muslimin*** campaign which was expressively aimed at reinforcing Daesh's military equipment, can be stored into digital values dark-wallets. Despite in many cases these money deposits or transfers can be traceable[92], with the emergence of alternative cryptocurrencies that are more opaque and better at concealing a user's activity (e.g. Dash, ZCash or Gram), these financial tools are going to give to jihadists movements a secure economic resource that can be potentially used to finance terrorist attacks abroad, buy weapons or strengthen their propaganda machine[93].

– **Extorsions, ransom and other illicit activities**: on May 20, 2018, a 13 years old boy was kidnapped in the town of Witbank in the eastern province of Mpumalanga, South Africa, by three men, demanding $123,000 worth (15 bitcoins) for his release[94]. In Ukraine, in 2017 on December 26, Pavel Lerner, a leading analyst and blockchain expert, was abducted and released after giving more than $1 million in bitcoins as ransom[95]. According to an agent speaking at a digital-asset industry conference in New York, the FBI has 130 cases tied to cryptocurrencies which of them, besides the

[88] Al Sadaqah Twitter page. Available at https://twitter.com/alsadaqah1

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

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

[91] An Arabic word referring to a charitable giving.

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

[93] The Meir Amit Intelligence and Terrorism Information Center (June 12, 2017) *Drive for bitcoin donations on an ISIS-affiliated website*. Available at https://www.terrorism-info.org.il/en/drive-bitcoin-donations-isis-affiliated-website/

[94] S. Busari (May 24, 2018) *The 13-year-old South African boy kidnapped for a bitcoin ransom has been found*. CNN. Available at https://edition.cnn.com/2018/05/24/africa/south-africa-bitcoin-ransom-boy-found/index.html

[95] P. Politiuk (December 29, 2017) *Ukraine kidnappers free bitcoin analyst after $1 million ransom paid*. Reuters. Available at https://uk.reuters.com/article/uk-ukraine-kidnapping/ukraine-kidnappers-free-bitcoin-analyst-after-1-million-ransom-paid-idUKKBN1EN1QE

cases related to drugs black-markets on the dark web, registered a significant rise in extortion schemes related to virtual currencies[96]. Moreover, approximately 25% of all bitcoin users and close to one-half of bitcoin transactions (44%) are associated with illegal activity[97]. Terrorist groups as Daesh or Al-Qaeda in West Africa have always been using methods as extortions, kidnapping (even on a daily basis) or human trafficking to generate considerable revenues and, the high skills they've proven to have in being flexible and always up to date in technological terms, could make harder to keep track of all their illicit revenues in these fields.

4.2 Lone-actors

This cluster represents individuals who are generally inspired by a central Islamic terrorist group without having a formal connection with it. As in the case of lone-wolves, these individuals are, in many cases, radicalized entirely online[98], without the need of being in contact with other followers, leaders of affiliated to the terrorist organization but mostly as the result (among other reasons usually related to marginalization, lack of self-recognition or psychopathologies) to a constant exposure to Islamic extremist online propaganda on the surface web, dark web and encrypted chats. Furthermore, as previously described, these people are usually extremely young and computer literate. These factors make them unpredictable (given the fact that they have not a direct connection with other jihadists online nor offline) and, being usually digital natives and very high-skilled in using modern technological tools, undetectable and with a high harmful potential.

The threat represented by lone-actors' use of cryptocurrencies could develop as follows:

– **Lone-wolves attacks equipment on the dark web**: there are several cases that highlight the dangerous threat of exploitation of crypto-values on the dark web black-markets. The Munich shooter, **Ali David Sonboly**, who bought a Glock 17 pistol and 350 round of ammunition on an e-commer-

[96] L. Katz, A. Massa (June 27, 2018) *FBI Has 130 Cryptocurrency-Related Investigations, Agent Says*. Bloomberg. Available at https://www.bloomberg.com/news/articles/2018-06-27/fbi-has-130-cryptocurrency-related-investigations-agent-says

[97] S. Foley, J.R. Karlsen, T.J. Putniņš (January 2018) *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?* University of Sydney – University of Technology Sydney – Stockholm School of Economics in Riga. Available at https://bit.ly/2GtHg5r

[98] C.S. Liang (May 02, 2018) *Dead or alive? The future of the Islamic State*. Geneva Center for Security Policy. Available at https://www.gcsp.ch/News-Knowledge/Global-insight/Dead-or-Alive-The-Future-of-the-Islamic-State#.WvQi7nQLSJI.linkedin

ce on the dark web by using bitcoins[99]. Mohammed Ali, 31, from Liverpool, who was diagnosed with mild Asperger's or autistic traits, bought five vials of ricin (enough to murder 1.400 people), under the online moniker of "**Weirdos 0000**", by using bitcoins, in 2015[100]. These are just two of a large number of cases related to the arms purchases (of any kind) on the dark web which highlight how easy for anyone has become to have access to dangerous items. Such weapons are smuggled in small quantities, sometimes just components that are later reassembled[101]. Hence the dark web has the potential to become the platform of choice for individuals (e.g. lone-wolves terrorists) to obtain weapons and ammunition behind the anonymity curtain provided by cryptocurrencies[102]. Furthermore, the increasing threat of lone-wolves using chemical weapons, as the 29-year-old Tunisian man, Sief Allah H, arrested in Cologne for producing ricin in his apartment or Waheba Issa Dais, a pro-IS Israeli woman, who attempted to provide detailed instructions on how to make ricin and then suggested the individual introduce the ricin to a government post or water reservoirs[103], should increase the awareness of dark web and lone-wolves nexus in order to be prepared to counter it.

– **Spread instructions aimed at using cryptocurrencies illegally**: as in the case of "***Bitcoin wa Sadaqat al-Jihad***" ("Bitcoin and the Charity of Jihad") which encouraged jihadists supporters to use digital currencies to finance ISIS and "limit economic support for infidels (Western Banks)" by giving instructions about how to use them[104], many other cases of lone actors

[99] K. Sengupta (August 26, 2016) *The Dark Web is a Dangerous New Frontier for Those who try to keep Terrorists a Bay*. Independent. Available at https://www.independent.co.uk/voices/germany-munich-attack-shooting-ali-david-sonboly-a7212151.html

[100] M. Robinson (September 18, 2015) *Breaking Bad-inspired computer geek who tried to buy enough ricin to kill 1,400 people from undercover FBI agent on hidden 'Dark Web' is jailed for eight years*. Mail Online. Available at http://www.dailymail.co.uk/news/article-3239810/Computer-geek-tried-buy-ricin-kill-1-400-people-undercover-FBI-agent-hidden-Dark-Web-jailed-eight-years.html

[101] J. Burke (April 18, 2018) *Military grade firearms increasingly available to terrorists in Europe – report*. The Guardian. Available at https://www.theguardian.com/world/2018/apr/18/arms-race-criminal-gangs-helping-terrorists-get-weapons-report-warns

[102] G. Persi Paoli, J. Aldridge, N. Ryan, R. Warnes (July 19, 2017) *International Arms Trade on the Dark Web*. RAND Corporation. Available at https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html

[103] Justice News (June 13, 2018) *Wisconsin Woman Charged With Attempting to Provide Material Support to ISIS*. The United States Department of Justice – Office of Public Affairs. Available at https://www.justice.gov/opa/pr/wisconsin-woman-charged-attempting-provide-material-support-isis

[104] *Bitcoin wa Sadaqat al-Jihad*. Available at https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf

which give information to finance terrorist organizations can be found on the dark web and encrypted chats. Furthermore, in case lone-jihadi-actors wouldn't have enough skills to perpetrate crimes with cryptocurrencies, as described in a 2016 report by Europol, they can rely on Crime-as-a-service (CaaS) available either on the deep web or on the dark web, where professional criminal or groups of criminals develop advanced tools, "kits" and other packaged services which are then offered up for sale or rent (by digital currencies) to other criminals who are usually less experienced[105].

– **Money laundering, scams and terrorism financing**: as already seen in the cases of **Zoobia Shahnaz**[106], who was financing IS by transferring money stolen by bank frauds in form of bitcoin and other cryptocurrencies, or **Ardit Ferizi**, an IS supporter who demanded payment in bitcoins from an Illinois Internet retailer, in exchange for removing bugs from its computers[107], there are signals that show an increasing trend in terrorism financing through online scams or money laundering. Some of these online money laundering methods, developed around transactions of small amounts of money, can take place inside the most unexpected web platform as, for instance, in the case of the exploitation of Massive Online Role Playing Games (MMORPG), as Second Life or World of Warcraft[108]. Or, keeping with the online scams, the case of the 19-year old Israeli-American hacker, arrested this March and convicted on June 28, who received payment in bitcoin (allegedly almost $250.000) by selling "intimidation" and extortion services to clients, charging (among other "services") $40 to make a call warning of a massacre in a private home; $80 to threaten a massacre at a school; and $500 to phone in a threat of a bomb on a plane[109].

[105] Institute for Economics and Peace (IEP) (2016) *Global Terrorism Index – Measuring and Understanding the Impact of Terrorism*. Available at http://economicsandpeace.org/wp-content/uploads/2016/11/Global-Terrorism-Index-2016.2.pdf

[106] The Meir Amit Intelligence and Terrorism Information Center (December 20, 2017) *Spotlight on global jihad*. Available at http://www.terrorism-info.org.il/en/spotlight-global-jihad-december-14-20-2017/

[107] T. Johnson (July 20, 2016) *Computer hack helped feed an Islamic State death list*. Mc Clatchy DC Bureau. Available at http://www.mcclatchydc.com/news/nation-world/national/article90782637.html

[108] J.L. Richet (2013). *Laundering Money Online: a review of cybercriminals' methods*. Tools and Resources for Anti-Corruption Knowledge, United Nations Office on Drugs and Crime (UNODC). Available at http://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf

[109] R. Hovel (June 28, 2018) *Israel Convicts Israeli-American Hacker Who Terrorized U.S. Jews With Bomb Threats*. Haaretz. Available at https://www.haaretz.com/israel-news/.premium-israeli-american-convicted-of-bomb-hoaxes-against-u-s-jewish-targets-1.6220106

5. Cyber jihad and terrorism financing: new methods – old rules

On July 2018, the **Financial Action Task Force (FATF)** published a report addressed to the G20 Finance Ministers and Central Banks Governors, summarizing the latest development in anti-money laundering and terrorism financing and drawing a short-term work program in these fields[110].

Regarding the **G20 member States,** the FATF points out that, due to a lack of a broadly shared international legal framework to regulate virtual currencies, it is still challenging to ensure a consistent global approach. The G20 Member States are still divided into those which are preparing laws or regulations to encourage financial and technological progress and those adopting measures mostly focused on prohibition. Hence, according to the FATF report, given the highly mobile nature of virtual currencies/crypto-assets, there is a risk of regulatory arbitrage or flight to unregulated safe havens. Furthermore, many national law enforcement authorities still have to improve their understanding of how to effectively conduct investigations of cases involving digital currencies, and how to disrupt criminals.

Another important feature of the report concerns an estimation of a growing **link between cryptocurrency and terrorism**, due to the evolution of either criminal or terrorist groups' financing means and capabilities. The 2018 FATF report, referring to the joint FATF/Egmont Group analysis on 106 case studies[111], demonstrates that third parties financial entities (especially Shell Companies) are a key feature in the **schemes designed to disguise money laundering or terrorism financing**, dividing them into three groups:

– Shell company: incorporated company with no independent operations, significant assets, ongoing business activities, or employees.
– Front company: fully functioning company with the characteristics of a legitimate business, serving to disguise and obscure illicit financial activity.
– Shelf company: incorporated company with inactive shareholders, directors, and secretary, left dormant for a longer period even if a customer relationship has already been established.

[110] FATF (2018) *FATF Report to G20 Finance Ministers and Central Bank Governors*. FATF, Paris, France. Available at www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-fm-cbg-july-2018.html

[111] FATF – Egmont Group (2018) *Concealment of Beneficial Ownership*. FATF, Paris, France. Available at www.fatf-gafi.org/publications/methodandtrends/documents/concealment-beneficial-ownership.html

5.1 The Dawa infrastructure, front organizations and the grey zone

Shell Companies and Front Companies (frequently non-profit organizations) cover a central role in terrorism propaganda, radicalization, recruitment, and terrorism financing. There are, indeed, various forms of radical Islam which pursue very far-reaching changes in society, but which do not involve the use of violence.

In these terms, referring to anti-money laundering or terrorism financing, a fundamental aspect to take into account is the broadly use made by terrorist groups of apparently licit **front organizations** or **religious centers** to disguise and launder their illegal financial activities: **the *Dawa* infrastructure**[112]. The *Dawa*'s main idea is based on the core belief that investing in educating Islamic values and social activity may bear fruit to broaden the base of public support in order to: expose Muslims and general public to **jihadi ideology**; provide international **logistic support**[113] to terrorists; grant a legal and legitimate **financial resource** for local or global Islamic leaders/organizations[114].

In some cases, the *Dawa* infrastructure is established around charity organizations (exploiting the Islamic values of charity donation: *zakāt* and *sadaqha*) which are publicly represented by non-profit companies, Islamic education centers, and hubs for fundraising events.

These front organizations are deeply connected at a public or political level[115] and represent one of the main provider of financial resources to terrorist groups, even compared to private companies and international or petty crime.

The features which make the global *Dawa* infrastructure one of the shadiest issue of terrorism financing is its unique ability to obscure its purposes either behind a public licit facade or by its ability to hide its illegal financial activities through the so-called "**grey zone**". The "grey zone" is the infrastructure that allows terrorist groups to cut the links between legal financial sources, channels used to transfer funds, and the financial aid to the *mujahideen*. A typical *modus operandi* which characterizes the "grey zone", is mo-

[112] S. Shay (2008) *Somalia Between Jihad and Restoration*. Taylor & Francis Group, New York .
[113] C.P. Clarke (August 28, 2017) *Hezbollah Has Been Active in America for Decades*. RAND Corporation. Available at https://www.rand.org/blog/2017/08/hezbollah-has-been-active-in-america-for-decades.html
[114] Israel Security Agency "Dawa" – *Hamas' Civilian Infrastructure and its Role in Terror Financing*. Available at https://www.shabak.gov.il/SiteCollectionImages/english/TerrorInfo/dawa-en.pdf
[115] G.R. Simpsons (March 18, 2003) *List of Early al Qaeda Donors Points to Saudi Elite, Charities*. The Wall Street Journal. Available at https://www.wsj.com/articles/SB104794563734573400

ving collected funds through a chain of transfers which are later withdrawn in cash to be further transported by couriers[116].

The *Dawa*'s politically correct approach is adopted also in online terrorism financing. In order to conceal the real purposes of fundraising and avoid blocking, online crowdfunding campaigns for the *mujahideen* often do not contain direct references to fundraising for terrorism financing but use ambiguous language or the pretext of collecting funds for charitable and humanitarian purposes.

Nevertheless, as explained in the International Institute for Counter-Terrorism (ICT) report on "2017 Trends in Cyberspace"[117], cryptocurrencies are introducing new forms of crowdfunding, making, in most cases, a clear distinction between crowdfunding online campaigns to finance terrorism behind a false intent and those made for explicit militaristic purposes.

– **Online charity crowdfunding campaigns**, more similar to the *Dawa* infrastructure politically correct approach (e.g. raise funds for the children of prisoners or to save a mosque from destruction) are carried out on both unregulated or mainstream social websites, where it is encouraged online interactions among users and which usually don't ask for donations by cryptocurrencies, but for other sort of means of online or cash payments[118].
– **Crowdfunding campaigns requiring donations in digital currencies** are more explicit about their terrorism financing purposes (e.g. Jahezona campaign explicitly showing that the donations were intended for buying weapons for terrorist groups). Hence, given an inadequate legal regulation on digital currencies, which still allows sending money in complete anonymity, terrorist organizations are using donation campaigns by cryptocurrency to ask for economic support for unambiguous and very clear militaristic ends. In fact, these campaigns don't encourage interaction among

[116] "Social network fundraising with prepaid card Individuals associated with ISIL called for donations via Twitter and asked the donors to contact them through Skype. Once on Skype, those individuals asked donors to buy an international prepaid card (a credit for mobile phone or the purchase of an Apple or other programs or credit for playing on the Internet) and send them the number of this prepaid card via Skype. Then, the fundraiser sent this card number to one of his followers in a neighbouring country from Syria, who would sell this card number at a lower price and give the cash proceeds to ISIL. Source: Saudi Arabia." FATF (2015). *Emerging Terrorist Financing Risks*. FATF, Paris, France. Available at www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

[117] International Institute on Counter-Terrorism (July 10, 2018) *Trends in Cyberspace*. IDC Herzliya. Available at https://www.ict.org.il/Article/2230/Trends_in_Cyberspace_Annual_Summary_2017#gsc.tab=0

[118] Excet for *Al Sadaqah* donation campaign. Available at http://www.itstime.it/w/bitcoin-and-other-types-of-cryptocurrency-modern-and-undetectable-ways-to-finance-terrorism-by-daniele-maria-barone/

users, but rather provide clear instructions on how to keep themselves as anonymous as possible.

5.2 Cryptocurrencies: Haram or Halal?

There is no evidence of transactions of relatively large amounts of money by cryptocurrency to finance Islamic terrorist groups, especially compared to the extensive illegal use of digital currencies perpetrated by small/global criminality or extremist political movements (as neo-Nazi groups[119]).

Indeed, the largest amount of money that terrorist groups raise from donations are those coming from false Islamic charity organizations through crowdfunding campaigns[120] or from wealthy donors from Gulf countries by direct money or gold donations[121]. These actors may have avoided a massive use of cryptocurrency to take part in the *jihad bil maal*[122] for reasons related to the instability of the digital-currencies market.

– **Economic reason**: even though investments in cryptocurrency have proved to be a profitable investment, its price volatility is keeping many investors from entering this new market. The recent bitcoin sharp hit on June 10 this year, as well as other virtual currencies, after South Korean cryptocurrency exchange Coinrail was hacked losing $ 42 million in value, is just one of the many cases that can increase the perception of how risky could be to transfer and store a large amount of money entirely online[123]. Furthermore, Islamic finance emphasizes economic activity mostly based on physical assets, avoiding interest payments and outright monetary speculation.

[119] As claimed by Royal United Services Institute (RUSI) associate fellow, David Carlisle "Where we probably see more significant adoption amongst extremist actors is amongst political extremists and particular amongst Neo-Nazi groups, who sometimes have an ideological affiliation with this notion of a borderless technology that allows one to operate outside the incumbent system and can be used as a manner of undermining the traditional banking system." N. Gutteridge (June 18, 2018) *Bitcoin terror threat ISIS terrorists and neo-Nazis using bitcoin and other cybercash to 'crowdfund' global propaganda, experts warn*. The Sun. Available at https://www.thesun.co.uk/news/6564841/isis-neo-nazis-bitcoin-funding-terror-propaganda/

[120] E. Kaplan (April 4, 2006) *Tracking Down Terrorist Financing*. Council on Foreign Relations. Available at https://www.cfr.org/backgrounder/tracking-down-terrorist-financing

[121] R. Windrem (September 21, 2014) *Who's Funding ISIS? Wealthy Gulf 'Angel Investors,' Officials Say*. NBC News. Available at https://www.nbcnews.com/storyline/isis-terror/who-s-funding-isis-wealthy-gulf-angel-investors-officials-say-n208006

[122] An Islamic principle according to which the Muslims who can't fight for the jihad, can contribute by giving money to support the *mujahideen*.

[123] J. Lockett, E. Hyatt (June 12, 2018) *Geek's gold. What is bitcoin, what's happened to the price and how can you buy the cryptocurrency?* The Sun. Available at https://www.thesun.co.uk/money/3000715/bitcoin-what-is-price-gbp-usd-today-value-cryptocurrency-buy/

– **Religious reason**: all Islamic scholars, given its price volatility, have always referred to cryptocurrency as a form of gambling, thus, *haram*[124]. Usually, terrorist front organizations and wealthy donors have to show their belonging to a strictly puritanical form of Islam to get recognition and be influential in the Islamic community, thus they're not allowed to have the same level of "ideological flexibility" that is typical of terrorist groups[125]. Nevertheless, because of FinTech companies not at all related to radical extremism but rather involved in a very legitimate and innovative business, which are interested in working in growing markets of the Middle East and Southeast Asia, cryptocurrencies are becoming more and more sharia-compliant and safer for Islamic investors.
– **Gold to stabilize cryptocurrencies' value**: a startup based in Dubai, OneGram[126], is spreading a new kind of gold-backed cryptocurrency. As Ibrahim Mohammed, OneGram co-founder, explained: "Gold was among the first forms of money in Islamic societies"[127]. Thus, OneGram is issuing a cryptocurrency structured in a way that each unit is backed by at least one gram of gold, giving far more stability to its value and obtaining a ruling that its cryptocurrency conforms with Islamic principles from **Dubai-based Al Maali Consulting**[128].
– **Sharia-compliant Californian FinTech firm**: California-based firm Stellar has received certification from **The Shariyah Review Bureau (SRB)**, a leading international Sharia advisory agency licensed by the Central Bank of Bahrain[129], for its blockchain platform and its native currency called Lumens[130], aiming at integrating the technology into the field of sharia-

[124] An Arabic word, which means "prohibited".

[125] Pro-Al-Qaeda English-language magazine Al-Haqiqa, distributed on Telegram, which, examining the Sharia permissibility of using bitcoin and similar currencies to fund jihad, stated: "We see lots of potential for the use of cryptocurrencies for our purposes." S. Stalinsky (March 30, 2018) *The Imminent Release Of Telegram's Cryptocurrency, ISIS's Encryption App Of Choice – An International Security Catastrophe In The Making*. MEMRI. Available at https://www.memri.org/reports/imminent-release-telegrams-cryptocurrency-isiss-encryption-app-choice-%E2%80%93-international

[126] Available at https://onegram.org/

[127] Al-Jazeera (April 8, 2018) *Islam and cryptocurrency*, halal *or not* halal? *The speculative nature of cryptocurrencies has triggered debate among Muslim scholars over its permissibility*. Available at https://www.aljazeera.com/news/2018/04/islam-cryptocurrency-halal-haram-180408145004684.html

[128] An Islamic finance consulting company.

[129] Available at http://shariyah.com/

[130] Available at https://www.stellar.org/lumens/

compliant financial products[131]. "Stellar is the first distributed ledger protocol to receive Sharia compliance certification in the money transfer and asset tokenization space...". This certification will allow the firm to work with "Islamic financial institutions in the Gulf Cooperation Council (i.e. Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, UAE) and parts of Southeast Asia (i.e. Indonesia and Malaysia)"[132].

6. A multidisciplinary approach to counter terrorism financing

As pointed out by Dr Peter R. Neumann on its paper *Don't Follow The Money*, "governments should integrate their efforts to restrict terrorist financing into their wider counterterrorism strategies instead of delegating this mission to finance ministries... actions aimed at countering terrorist funding may involve the financial system, but on other occasions, governments should use the military and law enforcement instead"[133].

Then, an intervention aimed at countering online terrorism financing implies the cooperation among apparently different sectors at a global level, which would allow filling the gap represented by four main macro-areas:

6.1 Lack of control over the online realm

By exploiting the surface and the deep web, Islamic terrorist organizations have the ability to either disseminate public messages or have a one-to-one type of communication with followers or sympathizers. Their economic resources in the online realm work in the same way of their online communication strategies: there are cases related to public links, in the most majority of them lightly-disguised, to fundraising campaigns or encrypted chats aimed to directly ask their followers an economic support. These aspects inevitably show a lack of control over online platforms[134] thus, the absence of a regulatory framework able to reduce the exploitation of the web by terrorist organiza-

[131] B. Vizcanio (July 17, 2018) *Cryptocurrency firm Stellar gets Islamic finance certification*. Reuters. Available at https://www.reuters.com/article/us-islamic-finance-cryptocurrencies/cryptocurrency-firm-stellar-gets-islamic-finance-certification-idUSKBN1K71RC

[132] Available at https://www.stellar.org/blog/stellar-receives-sharia-compliance-certification-transfers-tokenization

[133] P.R. Neumann (July/August 2017) *Don't Follow the Money – The Problem With the War on Terrorist Financing*. Foreign Affairs. Volume 96 – Number 4. Available at http://icsr.info/wp-content/uploads/2017/06/Foreign-Affairs-Dont-Follow-the-Money-Peter-R.-Neumann.pdf

[134] K. Leetaru (May 15, 2018) *The Problem With Using AI To Fight Terrorism On Social Media*. Forbes. Available at https://www.forbes.com/sites/kalevleetaru/2018/05/15/the-problem-with-using-ai-to-fight-terrorism-on-social-media/#4d640ad86fed

tions in terms of communication, is inevitably pouring onto the impossibility to detect terrorism's online economic resources.

Furthermore, the increasing developments of modern technologies in the financial sector are forcing governments to constantly try to understand and adapt to them as fast as they can, in order to avoid risks and threats to legality.

A more collaborative industry-government partnership could bring faster results in countering terrorist use of virtual currencies. In fact, this lack of cooperative measures and schemes, which can be noticed even in the most recent governmental decisions, could slowdown financial innovation without even decisively cut terrorist economic resources.

Cooperation could bring a more cohesive system, able to promote new and effective solutions to counter-terrorism financing while still encouraging progress in the financial or technological sector.

This could represent a primary condition to ensure that institutions will not have to keep on adapting their policies to modern technological improvements, innovative companies will not have to operate into a grey legal area, and terrorist organizations will not find an ideal ecosystem to perpetrate their illegal activities.

6.2 The ideological factor

The ability that terrorist groups have to turn even the most practical issues into a religious rule is quite a unique feature of these sort of organizations. Fundraising campaigns for *sadaqah* or extortions under the principle of *zakāt* or presenting the use of cryptocurrencies "for ideological-religious reasons"[135], are just some examples of how they can convince people to strengthen them financially while emphasizing their ideological narrative. Fundamentally terrorism is communication, thus Counter-narratives, Alternative Narratives, and Government Strategic Communications[136] have to be added to a strategy aimed to stop terrorist propaganda and prevent people from taking part in their fundraising campaigns.

[135] *Bitcoin wa Sadaqat al-Jihad*. Available at https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf

[136] A. Reed, H.J. Ingram, J. Whittaker (November 22, 2017) *Countering Terrorist Narratives*. Policy Department for Citizen's Rights and Constitutional Affairs – Directorate General for Internal Policies of the Union. Available at https://icct.nl/wp-content/uploads/2017/11/Reed-Ingram-Whittaker-Narratives.pdf

6.3 A global counter-terrorism strategy

The global reach of modern terrorism is developing a new warfare scenario which imposes on governments and supranational institutions a multidisciplinary approach that has to be reinforced by a transnational level of cooperation[137]. Terrorist groups have understood how to exploit their global networks either with organized crime or with like-minded terrorist organizations, making full use of transversal methods and skills able to reinforce their ranks and their funding. this is not yet enough to precisely detect and prevent cyber-jihadist activities. One of the reasons can be found in the fact that the possibilities to exploit cryptocurrencies for illegal activities are countless and many times can be very inclusive and imaginative.

Global terrorism, and especially Daesh after shifting from the management of the physical caliphate to a decentralized "virtual caliphate"[138], has brought a new protagonist in the hybrid warfare: the Lone-Wolve. Just as Lone-Wolves, the cyber-jihadists lone-actors are generally young and motivated subject, that can increase their motivation and operational capabilities directly in the online realm, by checking a few websites on the surface web or by searching for like-minded people which can help them reach Islamic extremist forums or chats or instructions in the dark web. Indeed, global terrorist groups and lone-actors seem to be more and more linked to each other by either a **top-down effect** of terrorist groups' propaganda, which is fragmentary able to radicalize people scattered across the globe, or by a **bottom-up effect**, which allows the terrorist groups to learn and use at their own advantage the modern methods or approaches brought up by their youngest followers. These actors, being fragmented and unpredictable, are able to spread more panic and fear than any terrorist organization itself.

Indeed, the HUMan INTelligence or COMmunication INTelligence seem to be still the most used sources to make the first steps to investigate suspicious terrorist activities which subsequently allow understanding the online network hidden behind some terrorist's actions[139]. But it should be taken into account that, the advantage represented by the increasing threat of these

[137] UN Meeting Coverage and Press releases (September 21, 2017) *Global Cooperation, Tackling Root Causes Central to Fight against Terrorism, World Leaders Stress on Third Day of General Debate*. United Nations. Available at https://www.un.org/press/en/2017/ga11950.doc.htm

[138] N. Spagna (December 5, 2017) *Daesh cambia forma. Resta (aumenta) la minaccia*. ITSTIME – Italian Team for Security, Terroristic Issues & Managing Emergencies. Available at http://www.itstime.it/w/daesh-cambia-forma-resta-aumenta-la-minaccia-by-nicolo-spagna/

[139] F. Tonacci (July 26, 2016) *Terrorismo, la rete criptata: così la cyber-jihad comunica con i lupi solitari in Europa*. La Repubblica. Available at http://www.repubblica.it/esteri/2016/07/26/news/terrorismo_rete_criptata_stato_islamico_cyber_jihad-144816976/

activities online (lone-actors' activity as well) is that they are always leaving a trace of what they do or of what they say. Thus, investigations should concentrate more efforts in strengthening their **Open Source Intelligence (OSINT)** methods, which is the key factor (with a strong and constant cooperation at local, State, and international level with the private sector[140]) to understand, fight and prevent this growing phenomenon.

Governments should increase their level of cooperation in order to reach those undetectable areas (both online (e.g. deep web, encrypted chats, cryptocurrencies) and offline (e.g. LDCs, marginalized people or communities) where terrorism finds fertile ground to proliferate. Hence, an improved and permanent cooperation at an international level with a cross-cutting competencies approach (e.g. military, sociological, economic, political, religious, digital) seems to be the only way to detect and decisively cut Daesh's financial resources.

6.4 Cryptocurrencies impose on authorities the duty to look at Islamic terrorists' real form

Global terrorism is not only made by decentralized groups scattered across the globe, small criminality, and borderline radical ideology but, as proven also by the *Dawa* infrastructure, it is also made by strong connections with political and religious influential figures and international entirely legal organizations. In these terms, Islamic terrorism should be analyzed as a cohesive entity which accurately calibrates each move in order to hit the *takfir* (infidels) as hard as possible while gathering public, political and religious support.

Same as the *Dawa* infrastructure, terrorism financing, can't be tackled only through the financial sector, but it is a subject which includes sociological, religious, political and military aspects[141].

Terrorist groups' connections not only with criminal organizations, but also with religious, political, and wealthy radical Islamic leaders or organization could be the missing piece of a broader religious and political justification that has, so far, kept global Islamic terrorist organizations from fully exploiting cryptocurrencies and digital assets.

[140] HM Government (June 2018) The United Kingdom's Strategy for Countering Terrorism. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

[141] P.R. Neumann (July/August 2017) *Don't Follow the Money – The Problem With the War on Terrorist Financing*. Foreign Affairs. Available at https://www.foreignaffairs.com/articles/2017-06-13/dont-follow-money

The developments in these terms should be accurately monitored to prevent Islamic terrorism from warping such a futuristic financial instrument as cryptocurrencies, into an unregulated fertile ground for terrorism financing.

As claimed by Dr. Jehangir Khan, Officer-in-Charge and Director of the Office of Counter-Terrorism at the UN: "Since 9/11 we have had numerous resolutions, numerous meetings in the security council and other forums, we have built a whole international legislative framework. A lot is being done, but if we look at the state of the world today... are we winning the war against terrorism or are we winning a few battles?"[142].

Of course, institutions are making progress in stopping online terrorism financing, but are we really able to counter its global reach?

References

A. Helmi, B.M. Hasbi, R. Mahzam (April 2018) *Cryptocurrencies: Potential For Terror Financing?* S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Available at https://www.rsis.edu.sg/rsis-publication/icpvtr/co18075-cryptocurrencies-potential-for-terror-financing/#.WyNd_RIzaqQ

A. Mizrahi (June 07, 2018) *Estonia Grants Licenses for Wallet and Exchange Services to Coinmetro*. bitcoin.com. Available at https://news.bitcoin.com/estonia-grants-licenses-for-wallet-and-exchange-services-to-coin-metro/

A. Reed, H.J. Ingram, J. Whittaker (November 22, 2017) *Countering Terrorist Narratives*. Policy Department for Citizen's Rights and Constitutional Affairs – Directorate General for Internal Policies of the Union. Available at https://icct.nl/wp-content/uploads/2017/11/Reed-Ingram-Whittaker-Narratives.pdf

A. Rosic (December 21, 2016) *What is Bitcoin Mining? A Step-by-Step Guide*. Huffington Post. Available at https://www.huffingtonpost.com/ameer-rosic-/what-is-bitcoin-mining-a-_b_13764842.html

Al Sadaqah Twitter page. Available at https://twitter.com/alsadaqah1

A. Sulleyman (January 24, 2018) *Bitcoin price is so high because criminals are using it for illegal trades, research suggests*. The Independent. Available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-fall-criminals-blockchain-anonymous-cryptocurrency-zcash-monero-dash-a8174716.html

Al-Jazeera (April 8, 2018) *Islam and cryptocurrency, halal or not halal? The speculative nature of cryptocurrencies has triggered debate among Muslim scholars over its permissibility*. Available at https://www.aljazeera.com/news/2018/04/islam-cryptocurrency-halal-halal-180408145004684.html

[142] International Institute for Counter-Terrorism (ICT) YouTube Channel (September 11, 2017) – *Officer-in-Charge and Director, Office of Counter-Terrorism, United Nations: From Rhetoric to Reality – Strengthening Multilateral Cooperation to Address the Growing Threat of Transnational Terrorism*. Available at https://www.youtube.com/watch?v=2WtlMgCgat4

Australian Government – AUSTRAC (April 11, 2018) *New Australian laws to regulate cryptocurrency providers*. Available at http://www.austrac.gov.au/media/media-releases/new-australian-laws-regulate-cryptocurrency-providers

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

B. Forrest, J. Scheck (February 20, 2018) *Jihadists See a Funding Boon in Bitcoin*. The Wall Street Journal. Available at https://www.wsj.com/articles/jihadists-see-a-funding-boon-in-bitcoin-1519131601

Bitcoin wa Sadaqat al-Jihad. Available at https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf

B. Marr (January 17, 2018) *A Complete Guide to Bitcoin in 2018*. Forbes. Available at https://www.forbes.com/sites/bernardmarr/2018/01/17/a-complete-beginners-guide-to-bitcoin-in-2018/#3484762b4418

B. Van Voris, C. Strohm (July 20, 2017) *Criminals' Online Market Targeted by U.S. After Founder Dies*. Bloomberg. Available at https://www.bloomberg.com/news/articles/2017-07-20/u-s-looks-to-seize-assets-tied-to-dark-web-site-alphabay

B. Vizcanio (July 17, 2018) *Cryptocurrency firm Stellar gets Islamic finance certification*. Reuters. Available at https://www.reuters.com/article/us-islamic-finance-cryptocurrencies/cryptocurrency-firm-stellar-gets-islamic-finance-certification-idUSKBN1K71RC

C. McCoogan (February 2, 2016) *Dark web browser Tor is overwhelmingly used for crime, says study*. The Telegraph – Technology Intelligence. Available at https://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/

Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – Financing of terrorism. Council of Europe. Available at https://www.coe.int/en/web/moneyval/implementation/financing-terrorism

C.P. Clarke (August 28, 2017) *Hezbollah Has Been Active in America for Decades*. RAND Corporation. Available at https://www.rand.org/blog/2017/08/hezbollah-has-been-active-in-america-for-decades.html

C.S. Liang (May 02, 2018) *Deaf or alive? The future of the Islamic state*. Geneva Center for Security Policy. Available at https://www.gcsp.ch/News-Knowledge/Global-insight/Dead-or-Alive-The-Future-of-the-Islamic-State#.WvQi7nQLSJI.linkedin

DeCenter YouTube Channel (December 22, 2017) *Telegram Open Network – TON* (Promo Final Version). Available at https://www.youtube.com/watch?v=3O-jnS-72gY4

Department of Justice – U.S. Attorney's Office – Eastern District of New York (December 14, 2017) *Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists. Defendant Stole and Laundered Over $85,000 Using Bitcoin and Other Cryptocurrencies*. Available at https://www.justice.gov/us-

ao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists

D. Gilbert (March 19, 2018) *Criminals are racing to cash out their bitcoin – Here's How They're Doing It*. Vice. Available at https://news.vice.com/en_ca/article/7xdzqa/criminals-are-racing-to-cash-out-their-bitcoin-heres-how-theyre-doing-it

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

E. Azani (March 06, 2018) *Global Jihad – The Shift from Hierarchal Terrorist Organizations to Decentralized Systems*. International Counter Terrorism Institute – Herzliya. Available at https://www.ict.org.il/Article/2210/Global_Jihad_Shift_from_Hierarchal_Terrorist_Organizations#gsc.tab=0

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

E. Kaplan (April, 4 2006) *Tracking Down Terrorist Financing*. Council on Foreign Relations. Available at https://www.cfr.org/backgrounder/tracking-down-terrorist-financing

E. Serravalle, E. Rosenberg (January 09, 2018) *Bitcoin can help terrorists secretly fund their deadly attacks*. FoxNews. Available at http://www.foxnews.com/opinion/2018/01/09/bitcoin-can-help-terrorists-secretly-fund-their-deadly-attacks.html

European Parliament Committees – Terrorism. Available at http://www.europarl.europa.eu/committees/en/terr/home.html

EUROPOL Press Release (June 28, 2018) *Police seize more than EUR 4.5 million in cryptocurrencies in Europe's biggest ever LSD bust*. Available at https://www.europol.europa.eu/newsroom/news/police-seize-more-eur-45-million-in-cryptocurrencies-in-europe%E2%80%99s-biggest-ever-lsd-bust

FATF (2015) *Emerging Terrorist Financing Risks*. FATF, Paris. Available at www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

FATF (2018) *FATF Report to G20 Finance Ministers and Central Bank Governors*. FATF, Paris, France. Available at www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-fm-cbg-july-2018.html

FATF – Egmont Group (2018) *Concealment of Beneficial Ownership*, FATF, Paris, France. Available at www.fatf-gafi.org/publications/methodandtrends/documents/concealment-beneficial-ownership.html

FATF/OECD (June 2015) *Guidance for a risk-based approach virtual currencies*. Available at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

Financial Technology Innovation and Defense Act 115th Congress – 2d Session (January 10, 2018) Available at https://www.congress.gov/bill/115th-congress/house-bill/4752/text?q=%7B%22search%22%3A%5B%22congressId%3A115+AND+-billStatus%3A%5C%22Introduced%5C%22%22%5D%7D&r=66

F. Tonacci (July 26, 2016) *Terrorismo, la rete criptata: così la cyber-jihad comunica con i lupi solitari in Europa*. La Repubblica. Available at http://www.repubblica.it/esteri/2016/07/26/news/terrorismo_rete_criptata_stato_islamico_cyber_jihad-144816976/

G.F. (January 27, 2014) *Cryptographic Currency – Washing virtual money*. The Economist. Available at https://www.economist.com/2014/01/27/washing-virtual-money

G. Persi Paoli, J. Aldridge, N. Ryan, R. Warnes (July 19, 2017) *International Arms Trade on the Dark Web*. RAND Corporation. Available at https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html

G.R. Simpsons (March 18, 2003) *List of Early al Qaeda Donors Points to Saudi Elite, Charities*. The Wall Street Journal. Available at https://www.wsj.com/articles/SB104794563734573400

Guide On How To Access The Silk Road 3.0 (3.1). Available at https://silkroaddrugs.org/guide-on-how-to-access-the-silk-road-3-0/

G. Weimann (November 3, 2016) *Terrorist Migration to the Dark Web*. Univeriteit Leiden – The Netherlands. Available at http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html

H. Alexander (December 14, 2017) *New York woman charged with sending $85,000 in bitcoin to support Isil*. The Telegraph. Available at https://www.telegraph.co.uk/news/2017/12/14/new-york-woman-charged-sending-85000-bitcoin-support-isil/

HM Government (June 2018) *The United Kingdom's Strategy for Countering Terrorism*. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

H. Nasser (January 09, 2018) *Exclusive: Telegram ICO (TON) Leaked Whitepaper Reveals Ambitious Plans*. CryptoVest. Available at https://cryptovest.com/news/exclusive-telegram-ico-ton-leaked-whitepaper-reveals-ambitious-plans/

https://coinmetro.com/about

http://www.kofiu.go.kr/eng/sub1/1.jsp

https://onegram.org/

http://shariyah.com/

https://www.stellar.org/blog/stellar-receives-sharia-compliance-certification-transfers-tokenization

https://www.stellar.org/lumens/

ICT Cyber-Desk Periodic Review (October-November 2013) *Cyber-Terrorism Activities Report No. 6*. IDC Herzliya – International Institute for Counter-Terrorism (ICT). Available at https://www.ict.org.il/UserFiles/Cyber%20Report%206.pdf

Il Sole 24 Ore (May 10, 2018) *Money transfer illegali per finanziare la Jihad: arrestati 14 fiancheggiatori*. Available at http://www.ilsole24ore.com/art/notizie/2018-05-10/terrorismo-arrestati-14-fiancheggiatori-formazioni-jihadiste-081156.shtml?uuid=AEGPd1lE

I.L. Tisnadibrata (September 01, 2017) *Indonesia Tracks Online Funding of Terror Groups*. Benar News. Available at https://www.benarnews.org/english/news/indonesian/online-payments-01092017155456.html

Institute for Economics and Peace (IEP) (2016) *Global Terrorism Index – Measuring and Understanding the Impact of Terrorism*. Available at http://economicsandpeace.org/wp-content/uploads/2016/11/Global-Terrorism-Index-2016.2.pdf

International Institute on Counter-Terrorism (July 10, 2018) *Trends in Cyberspace*. IDC Herzliya. Available at https://www.ict.org.il/Article/2230/Trends_in_Cyberspace_Annual_Summary_2017#gsc.tab=0

International Institute for Counter-Terrorism (ICT) YouTube Channel (September 11, 2017) – Officer-in-Charge and Director, Office of Counter-Terrorism, United Nations: From Rhetoric to Reality – Strengthening Multilateral Cooperation to Address the Growing Threat of Transnational Terrorism. Available at https://www.youtube.com/watch?v=2WtlMgCgat4

Israel Security Agency "*Dawa" – Hamas' Civilian Infrastructure and its Role in Terror Financing*. Available at https://www.shabak.gov.il/SiteCollectionImages/english/TerrorInfo/dawa-en.pdf

I. von Behr, A. Reding, C. Edwards, L. Gribbon (2013) *Radicalization in the digital era. The use of the internet in 15 cases of terrorism and extremism*. RAND Europe. Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

J. Burke (April 18, 2018) *Military grade firearms increasingly available to terrorists in Europe – report*. The Guardian. Available at https://www.theguardian.com/world/2018/apr/18/arms-race-criminal-gangs-helping-terrorists-get-weapons-report-warns

J. Dirnhuber (August 29, 2018) *Funding hate – ISIS fanatics plundered bank accounts of Brit couple murdered by jihadis in South Africa and used money to buy bitcoin and fund jihadi training camp*. The Sun. Available at https://www.thesun.co.uk/news/7122832/rod-saunders-rachel-isis-bank-accounts-terror-south-africa/

J. Lockett, E. Hyatt (June 12, 2018) *Geek's gold. What is bitcoin, what's happened to the price and how can you buy the cryptocurrency?*. The Sun. Available at https://www.thesun.co.uk/money/3000715/bitcoin-what-is-price-gbp-usd-today-value-cryptocurrency-buy/

J.L. Richet (2013). *Laundering Money Online: a review of cybercriminals' methods. Tools and Resources for Anti-Corruption Knowledge*. United Nations Office on Drugs and Crime (UNODC). Available at http://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf

J. Sagar (November 14, 2015) *Bitcoin 3 Million Dollars*. News BTC. Available at https://www.newsbtc.com/2015/11/14/isil-militants-linked-to-france-terrorist-attacks-had-a-bitcoin-address-with-3-million-dollars/

Justice News (June 13, 2018) *Wisconsin Woman Charged With Attempting to Provide Material Support to ISIS*. The United States Department of Justice – Office of Public Affairs. Available at https://www.justice.gov/opa/pr/wisconsin-woman-charged-attempting-provide-material-support-isis

J. Warrick (December 23, 2016) *The 'app of choice' for jihadists: ISIS seizes on Internet tool to promote terror*. The Washington Post. Available at https://www.washingtonpost.com/world/national-security/the-app-of-choice-for-jihadists-isis-seizes-on-internet-tool-to-promote-terror/2016/12/23/a8c348c0-c861-11e6-85b5-76616a33048d_story.html?utm_term=.0a8b5bf40b52

K. Helms (January 30,2018) *South Korea Ends Anonymous Cryptocurrency Trading Today*. bitcoin.com. Available at https://news.bitcoin.com/south-korea-ends-anonymous-cryptocurrency-trading/

K. Leetaru (May 15, 2018) *The Problem With Using AI To Fight Terrorism On Social Media*. Forbes. Available at https://www.forbes.com/sites/kalevleetaru/2018/05/15/the-problem-with-using-ai-to-fight-terrorism-on-social-media/#4d640ad86fed

Krypt3ia (October 14, 2013) *Darknet Jihad*. Available at https://krypt3ia.wordpress.com/2013/10/14/darknet-jihad/

K. Sengupta (August 26, 2016) *The Dark Web is a Dangerous New Frontier for Those who try to keep Terrorists a Bay*. Independent. Available at https://www.independent.co.uk/voices/germany-munich-attack-shooting-ali-david-sonboly-a7212151.html

L. Dearden (July 12, 2017) *UK residents donate thousands of pounds a year to Islamist extremist organisations, Home Office reveals*. Independent. Available at https://www.independent.co.uk/news/uk/home-news/british-people-islamist-funding-extremist-organisations-home-office-amber-rudd-uk-isis-terrorism-a7837451.html

L. Katz, A. Massa (June 27, 2018) *FBI Has 130 Cryptocurrency-Related Investigations, Agent Says*. Bloomberg. Available at https://www.bloomberg.com/news/articles/2018-06-27/fbi-has-130-cryptocurrency-related-investigations-agent-says

M. Bihter (2011) *Money Laundering And Terrorism As A Global Threat And A Comparison Between United States And Turkey*. Ankara Bar Review. Available at http://www.ankarabarosu.org.tr/siteler/AnkaraBarReview/tekmakale/2011-2/6.pdf

M. Del Castillo (December 21, 2017) *Think Tank Links Rising Bitcoin Price to Terrorist Use*. Coindesk. Available at https://www.coindesk.com/u-s-think-tank-finds-rising-bitcoin-price-linked-terrorist-interest/

MEMRI Cyber & Jihad Lab (November 13, 2017) *Online Campaign In English Raising Funds For The Jihad In Syria In bitcoin*. MEMRI. Available at http://cjlab.memri.org/latest-reports/online-campaign-in-english-raising-funds-for-the-jihad-in-syria-in-bitcoin/

M. Jain (December 14, 2017) *How to use everyday accounting tools to understand cryptocurrency*. HBX Business Blog – Harvard Business School. Available at https://hbx.hbs.edu/blog/post/how-to-apply-everyday-accounting-tools-to-understand-cryptocurrency?utm_source=linkedin&utm_medium=social&utm_campaign=FA

M. Robinson (September 18, 2015) *Breaking Bad-inspired computer geek who tried to buy enough ricin to kill 1,400 people from undercover FBI agent on hidden 'Dark Web' is jailed for eight years*. Mail Online. Available at http://www.dailymail.co.uk/news/article-3239810/Computer-geek-tried-buy-ricin-kill-1-400-people-undercover-FBI-agent-hidden-Dark-Web-jailed-eight-years.html

M. Sabella (January 01, 2018) *Bitcoin, il Mufti del Cairo lancia una fatwa contro la criptovaluta*. Corriere della Sera. Available at https://www.corriere.it/economia/18_gennaio_01/bitcoin-mufti-cairo-lancia-fatwa-contro-criptovaluta-a7c062d0-ef18-11e7-97e1-31c2bf5f7cef.shtml

M. Zencho (August 17, 2017) *Bitcoin for Bombs*. Council on Foreign Relations. Available at https://www.cfr.org/blog/bitcoin-bombs

N. Gutteridge (June 18, 2018) *Bitcoin terror threat ISIS terrorists and neo-Nazis using bitcoin and other cybercash to 'crowdfund' global propaganda, experts warn*. The Sun. Available at https://www.thesun.co.uk/news/6564841/isis-neo-nazis-bitcoin-funding-terror-propaganda/

N. Malik (May 2018) *Terror In the Dark. Centre of the Response to Radicalization and Extremism*. Available at http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

N. Popper (October 1, 2017) *What is Bitcoin and How Does It Work?* The New York Times. Available at https://www.google.it/amp/s/mobile.nytimes.com/2017/10/01/technology/what-is-bitcoin-price.amp.html

N. Spagna (December 5, 2017) *Daesh cambia forma. Resta (aumenta) la minaccia*. ITSTIME – Italian Team for Security, Terroristic Issues & Managing Emergencies. Available at http://www.itstime.it/w/daesh-cambia-forma-resta-aumenta-la-minaccia-by-nicolo-spagna/

O. Kharif, M. Leising (January 29, 2018) *Bitcoin and Blockchain*. Bloomberg. Available at https://www.bloomberg.com/quicktake/bitcoins

P.M. Jost, H.S. Sandhu (January 2000) *The hawala alternative remittance system and its role in money laundering*. United States Department of the Treasury Financial Crimes Enforcement Network (FinCEN) in cooperation with INTERPOL/FOPAC. Available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-Hawala-rpt.pdf

P. Politiuk (December 29, 2017) *Ukraine kidnappers free bitcoin analyst after $1 million ransom paid*. Reuters. Available at https://uk.reuters.com/article/uk-ukraine-kidnapping/ukraine-kidnappers-free-bitcoin-analyst-after-1-million-ransom-paid-idUKKBN1EN1QE

P.R. Neumann (July/August 2017) *Don't Follow the Money – The Problem With the War on Terrorist Financing*. Foreign Affairs. Volume 96 – Number 4. Available at http://icsr.info/wp-content/uploads/2017/06/Foreign-Affairs-Dont-Follow-the-Money-Peter-R.-Neumann.pdf

R. Basra, P.R. Neumann, C. Brunner (2016) *Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus*. The International Center for Studies on Radicalization and Political Studies. Available at http://icsr.info/wp-content/uploads/2016/10/Criminal-Pasts-Terrorist-Futures.pdf

R. Hovel (June 28, 2018) *Israel Convicts Israeli-American Hacker Who Terrorized U.S. Jews With Bomb Threats*. Haaretz. Available at https://www.haaretz.com/israel-news/.premium-israeli-american-convicted-of-bomb-hoaxes-against-u-s-jewish-targets-1.6220106

R. Windrem (September 21, 2014) *Who's Funding ISIS? Wealthy Gulf 'Angel Investors,' Officials Say*. NBC News. Available at https://www.nbcnews.com/storyline/isis-terror/who-s-funding-isis-wealthy-gulf-angel-investors-officials-say-n208006

Satoshi Nakamoto (pseudonym used by the anonymous bitcoin developer) *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at https://bitcoin.org/bitcoin.pdf

S. Busari (May 24, 2018) *The 13-year-old South African boy kidnapped for a bitcoin ransom has been found*. CNN. Available at https://edition.cnn.com/2018/05/24/africa/south-africa-bitcoin-ransom-boy-found/index.html

Security Council Counter-Terrorism Committee (April, 30 2018) CTED *Executive Director participates in international conference on terrorism financing*. Available at https://www.un.org/sc/ctc/news/2018/04/30/cted-executive-director-participates-international-conference-terrorism-financing/

S. Foley, J.R. Karlsen, T.J. Putniņš (January 2018) *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?* University of Sydney – University of Technology Sydney – Stockholm School of Economics in Riga. Available at https://bit.ly/2GtHg5r

S. Shay (2008) *Somalia Between Jihad and Restoration*. Taylor & Francis Group, New York.

S. Stalinsky (March 30, 2018) *The Imminent Release Of Telegram's Cryptocurrency, ISIS's Encryption App Of Choice – An International Security Catastrophe In The Making*. MEMRI. Available at https://www.memri.org/reports/imminent-release-telegrams-cryptocurrency-isiss-encryption-app-choice-%E2%80%93-international

(June 12, 2018) *South Korea to Impose Stricter Regulation of Cryptocurrency Exchanges*. Sputnik. Available at https://sputniknews.com/science/201806121065344133-south-korea-regulation-crypto-exchanges/

TE SAT European Union (2017) *Terrorism Situation and Trend Report 2017*. Available at https://www.europol.europa.eu/tesat/2017/

The Meir Amit Intelligence and Terrorism Information Center (December 06, 2017) *Drive for bitcoin donations on an ISIS-affiliated website*. Available at http://www.terrorism-info.org.il/en/drive-bitcoin-donations-isis-affiliated-website/

The Meir Amit Intelligence and Terrorism Information Center (2018) I*n view of its financial problems, ISIS is selling coins that it minted at the time of the Islamic State. Payment for the coins is made via an international clearing system*. Available at http://www.terrorism-info.org.il/app/uploads/2018/01/E_003_18.pdf

The Meir Amit Intelligence and Terrorism Information Center (December 14-20, 2017) *Spotlight on global jihad*. Available at http://www.terrorism-info.org.il/en/spotlight-global-jihad-december-14-20-2017/

T. Johnson (July 20, 2016) *Computer hack helped feed an Islamic State death list*. Mc Clatchy DC Bureau. Available at http://www.mcclatchydc.com/news/nation-world/national/article90782637.html

T. Keatinge (December 12, 2014) *Finances of jihad: How extremist groups raise money*. BBC News. Available at http://www.bbc.com/news/world-middle-east-30393832

T. Keatinge, D. Carlisle, F. Keen (May 2018) *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs. Available at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

T.L. Quintero (September 13, 2017) *The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime*. *InSight Crime*. Available at https://www.insightcrime.org/news/analysis/connected-black-market-how-dark-web-empowered-latam-organized-crime/

(July 21, 2017) *Two of the biggest dark-web markets have been shut down – History suggests that other sites will soon fill the void*. The Economist. Available at https://www.economist.com/graphic-detail/2017/07/21/two-of-the-biggest-dark-web-markets-have-been-shut-down

UN Meeting Coverage and Press releases (September 21, 2017) *Global Cooperation, Tackling Root Causes Central to Fight against Terrorism, World Leaders Stress on Third Day of General Debate*. United Nations. Available at https://www.un.org/press/en/2017/ga11950.doc.htm

W. Dai (1998) *B-Money*. Available at http://www.weidai.com/bmoney.txt

W. Zhao (January 17, 2018) *Proposed US Task Force Would Tackle Crypto Use in Terrorism Financing*. CoinDesk. Available at https://www.coindesk.com/proposed-us-task-force-would-tackle-crypto-use-in-terrorism-financing/

Y. Fanusie (August 24, 2016) *The New Frontier in Terror Fundraising: Bitcoin*. The Cipher Brief. Available at https://www.thecipherbrief.com/column/private-sector/the-new-frontier-in-terror-fundraising-bitcoin

Y.J. Bob (January 28, 2018) *ISIS, other jihadists increade bitcoin use after fall of Caliphate*. The Jerusalem Post. Available at https://www.jpost.com/Middle-East/ISIS-Threat/ISIS-other-jihadists-increase-bitcoin-use-after-fall-of-Caliphate-540079

Z.K. Goldman, E. Maruyama, E. Rosenberg, E. Saravalle, J. Solomon-Strauss (May 2017) *Terrorist Use of Virtual Currencies: Containing the Potential Threat*. Center for a New American Security (CNAS). Available at https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-TerroristFinancing-Final.pdf

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: 978-88-9335-387-8

Euro 20,00