INTERNATIONAL CONFERENCE RCIC'17
Redefining Community in Intercultural Context
Bari, 5-6 June 2017

MODERN METHODS OF FINANCING TERRORISM IN A GLOBAL AND INTERCULTURAL SOCIETY: *CRYPTO-CURRENCY*

Cristina CARATA

"Mihai Viteazul" National Intelligence Academy, Bucharest, Romania

Abstract: *In the global and intercultural society we live in today, cyber security has become, in the last twenty years, an important subject on the agenda of states worldwide due to the growing number of technical innovation and the way they are "monopolizing" an increasingly large part of our lives, whether we talk about personal data, industrial espionage or access to sensitive information. The article examines the way crypto-currencies can be used as a new method for financing terrorism, in the 21st century, given the ongoing changes, challenges and oportunities of the society we currently live in, especially regarding the cyber security area. The paper provides a short analysis of how crypto-currencies were created, how they work and the way different states relate to this expanding phenomenon in an attempt to understand why they represent an "attraction" for terrorist activities, with a focus on their primary characteristics such as anonymity for transactions and users, fast transactions and reliability. Capitalizing the experiences and lessons learnt so far from the analysis of the traditional methods of financing terrorism, the paper focuses on key dimensions like: the way new payment technologies pose an emerging vulnerability that may increase over time and the global policies and legal framework that should emerge due to this phenomenon as well as the new digital realities imposed by it, in a society that is becoming global due to technology. At the same time, increased attention should be paid to the need of moving forward towards the new paradigm of the modern cyber security and intelligence and also to the role of technology as a key factor present in all stages of society today.*

Keywords*: technology**; terrorism financing; cyber security; crypto-currency*

1. INTRODUCTION

In today's modern society, technology has advanced so much that it is present everywhere in our lives. We can assert, without restraint, that it undoubtedly holds the most important role in influencing contemporary life. In a field such as the technological one, where evolution is happening rapidly, sometimes from day to day and much of the media and the general public's attention is focused on the latest inventions, gadgets and innovations launched, an estimate of future developments is rather complicated.

Although in the vast majority of cases the spread of state-of-the-art technologies in all areas offers visible benefits, as a side effect, we can discuss about the emergence of potential security threats and vulnerabilities, creating problematic security paradigms.

> With the development of modern technologies, the interest in the security area represents the emergence of the notion of "cybernetic space", which, due to its characteristics (low connection costs, anonymity and potential asymmetric vulnerabilities) has generated new vulnerabilities and security risks. Cyber attacks have become increasingly frequent, both at an interstate level (…) as well as in state-to-people relations (hacker attacks on government sites and strategic economic, military and political institutions). (…) Facing all these realities, ensuring cyber security has become a major concern for all actors involved, both at an institutional level - where the responsibility for the development and implementation of coherent policies in the field is, as well as for private entities interested in protecting their own patrimony and intellectual property. Most states have taken steps to strengthen the capability of cyber defense, including adopting a specific legal framework (Mâță, 2016:38).

The continuous progress of technology and the notion of "cybernetic space" did not bypass the phenomenon of terrorism, which has gained increasing importance over the last years, in cross-border dimensions. The dynamics of the global

terrorist phenomenon is constantly changing not only through the obvious changes in its motivations - which have become very diverse, from political and religious motives to economic or cybernetic - but also through the methods used, methods that have adapted to the global technological society.

Among the methods used by terrorist networks to exploit the cybernetic space - like cyber attacks, online propaganda or collecting open-source information – financing terrorist operations with the help of emerging technologies is a key point on the agenda of all such organizations around the world. The success of a terrorist group, like any other criminal group, is to be able to build and maintain an effective financial infrastructure. For this, they need to develop sources of funding (the methods can range from online fundraising, selling online propaganda material or obtaining *crypto-currency*), money laundering and, ultimately, ways to ensure that these funds are used to obtain the logistics needed to commit terrorist acts (Martimof, 2010).

While maintaining the same trend of alignment with global society, terrorist financing has acquired modern valences. According to the FATF-Financial Action Task Force,

> terrorists constantly adjust how and where they move their funds to circumvent safeguards that countries have put in place. They will use new technologies or products such as social media payments to attract and move their money. Understanding how a terrorist organization raises, moves and uses its funds is critical to choking the funds and disturbing their atrocities (Financial Action Task Force, 2016).

Crypto-currency is among the modern technologies used by terrorist organizations to provide the necessary funds for organizing attacks. Nevertheless a growing phenomenon, an analysis of this new digital payment instrument is required to determine to what extent it represents an "attraction" for terrorist groups.

2. WHAT IS *CRYPTO-CURRENCY*?

According to the European Commission's legislative proposals of July 2016 on money laundering, tax evasion and terrorist financing, *crypto-currency* can be defined as

> (…) a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically (European Commission, 2016).

Also, the European Central Bank, in its 2015 "Virtual currency schemes – a further analysis" Report, refers to virtual currencies as follows:

> the ECB does not regard virtual currencies, such as *Bitcoin*, as full forms of money as defined in economic literature. Virtual currency is also not money or currency from a legal perspective. For the purpose of this report, it is defined as a digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money (European Central Bank, 2015).

Prior to this, in 2012, the same institution has defined *crypto-currencies* as

> a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community (European Central Bank, 2012).

In technical terms, *crypto-currency* or virtual currency is a non-banking and decentralized method (supported by its users) to exchange value between individuals, peer-to-peer (bidirectional, without intermediary) and based on cryptographic protocols and proof-of-work protocols (based on hashing algorithms) as securing methods.

3. THE HISTORY OF MODERN *CRYPTO-CURRENCY*

The first *crypto-coin* was *Bitcoin,* which is currently the most known and referential term in the field. The concept of "*bitcoin*" appeared in 2008 in the document "Bitcoin: A Peer-to-Peer Electronic Cash System", published under the pseudonym Satoshi Nakamoto (the real name or identity is still unknown to this day). In January 2009, the author of the document created the first part of *Bitcoin*, calling it the Genesis block and shortly after presented the project to a group of cryptographic experts.

Until 2010, *Bitcoin* has never been used for transactions but, by that time, a community of programmers revised the code along with Satoshi Nakamoto, launching version 0.2 and improving the previous one. The first *Bitcoin* transaction for a good took place on May 21st, 2010 when a *Bitcoin* user, named Laszlo, bought a 25-U.S. dollars pizza using 10000 *Bitcoins* (Mitran, 2014). After this milestone, the first major increase in *Bitcoin* took place in July of the same year after it was

mentioned in an article on the SlashDot technology site. Thus, transactions increased and *Bitcoin* tightened its value, reaching 0.08 U.S. dollars from 0.008 U.S. dollars. At the beginning of 2011, *Bitcoin* had already reached 0.50 U.S. dollars, and, in the middle of the year, it was mentioned in the "Time" magazine - as a result, in June it was worth 10 U.S. dollars. A rather spectacular growth can be observed, due largely to the media. At the end of 2013, the value of a *Bitcoin* reaches a new record of 267 U.S. dollars and since then the value is rising, reaching around 1500 U.S. dollars, as we speak. As a result of *bitcoin*'s success, over 700 types of *crypto-coins,* called *Altcoins,* are now available on the market, but only about 20 of them have exceeded a trading threshold of 10 million U.S. dollars. These *Altcoins* include *Ethereum, Ripple, Litecoin, Monero, Dash or Augur*.

The prospects for increasing the number of virtual coins are developing due to their popularity and media coverage. To understand the size of the phenomenon, in late 2012, WordPress became the first major merchant to accept payment in *Bitcoin*. Others, including Newegg.com (an online electronics retailer), Expedia and Microsoft, followed. More and more online merchants accept *crypto-currency,* especially *bitcoin,* as a legitimate payment method.

4. HOW DOES *CRYPTO-CURRENCY* WORK?

Based on several decades of cryptography research, *Bitcoin* (BTC), a reference system for the *crypto-coin* phenomenon, includes four major innovations combined in an extremely ingenious way: a peer-to-peer decentralized network: this is the BTC protocol (a peer-to-peer decentralized network for *crypto-coins* is a computer network made up of several nodes, none of which are central. In other words, they do not depend on a central entity and nobody has absolute control over the network); a public register for the transactions: blockchain; a decentralized, deterministic and well modeled mathematical mechanism for issuing new *Bitcoin*: mining; a decentralized transaction verification system: transaction script (Dumitru, 2015). The *Bitcoin* system - a reference system for the *crypto-coin* phenomenon - relies on a peer-to-peer network and asymmetric cryptography, as basic features, besides the innovations mentioned above.

In simple terms, asymmetric cryptography uses a pair of asymmetric keys, one public (that encrypts a text) and one private (that decodes the encrypted text and creates a digital signature) in order to confirm different transactions. In the case of *Bitcoin* transactions, asymmetric cryptography ensures anonymity and confidentiality. The principles of this system are described in the original document published by Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”.

After understanding the mechanism behind the *bitcoin* system, of interest for the subject covered by this article is obtaining and trading *crypto-currency* - *bitcoin* or others, because the system operating roughly the same for all types of coins. First and foremost, in order to obtain or to trade any form of virtual currency, the first necessary step is an "electronic wallet" or "digital wallet" (e.g. *bitcoin* wallets). The concept of "digital wallet" is somehow similar to that of a bank account but with some notable differences. In short, an electronic wallet is an application (software or hardware) that connects to the virtual currency network and allows it to be managed and traded with other users. There are several types of electronic wallets (software, hardware, brain wallets, cold wallets, etc.), but their operating principle is the same: they generate unique addresses that can be used to receive, store and transmit virtual coins. There is no address limit: any user can generate and use as many as possible. So, the digital wallet is a necessary step for trading trade virtual coins. There are, however, several ways to obtain virtual coins, namely: they can be bought from the so-called "exchanges" (changing legal tender in *bitcoins*, for example), they can be transferred between proximity users or created through the method called "mining":

- Getting virtual coins through exchanges: as with classic currency exchange houses, virtual currency exchanges allow their users to convert legal tender into *crypto-currency*, in a specific manner (that includes trading with other users);
- Virtual currency transfer between proximity users: virtual coins can be exchanged (or virtual currency can be exchanged for legal tender) on different dedicated platforms (e.g. www.localbitcoins.com) by swapping between users. This type of trading is also known as "over-the-counter (OTC) trading." All trades are conducted between users directly;
- Mining: *Crypto-coins* can be bought, as we have shown above, but they can also be created. In short, the mining process implies that users use a specific mining program that solves different algorithms in order to release blocks of coins into the network (in circulation). Dedicated mining programs are installed on performing computers (the rate of return on a personal computer is extremely small, so an initial investment of about $ 5,000 is required for hardware and software

equipment that will allow a profitable mining rate. This initial investment must also take into account the electricity consumption - computers must "mine" 24 hours a day and have a competent cooling system).

After obtaining the digital wallet and the *crypto-coins*, the next step is to trade them. *Crypto-currency* transactions are secured using cryptography between virtual wallets (a "private key" is assigned to each virtual wallet in order to avoid the modification of the transaction by other users and to secure it). Also, each transaction with virtual coins is registered in an "electronic register", but the name of the buyer and seller is not registered - only the wallet ID. This feature of digital currency transactions - the anonymity of the users - is what makes them so attractive to be used in illegal activities.

5. THE MAIN CHARACTERISTICS OF *CRYPTO-CURRENCY*

When the first functional *crypto-coin, bitcoin,* emerged in 2009, there were not many who gave it a chance to survive and looked at this technological appearance with skepticism. However, nowadays - and only 8 years after the *bitcoin* emerged- the phenomenon has grown to such an extent that there are well-known sites (such as Wordpress, Amazon, Expedia, or Microsoft) that accept payment for various products or services in virtual currency, banking institutions analyze the possibility of using *crypto-currency* and the technology behind it for their own benefit, governmental institutions across the globe are studying the phenomenon and trying to regulate it and, moreover, even the idea of issuing a national *crypto-currency* based on the blockchain technology, in countries like South Africa, Greece or even China, is being discussed.

Cripto-currency has brought to light new concepts, some of them even innovative - unknown to this date in the currency field - that can fundamentally change the way we look at the payment systems. Based on the definition and bases of virtual coins functioning, previously set out in this article, the features of these new financial instruments that can become "appealing" to terrorist groups can be detached.

Firstly, *crypto-coins* do not exist in physical form (they are digital coins without a classical representation in physical form) and, most importantly, they are a decentralized payment form. So, they are not created or controlled by any governmental institution, nor regulated. Therefore, classical measures that may apply to criminal offenses, such as examining or blocking accounts, can not be applied. Because of this feature, *crypto-coins* are, at the moment, out of the traditional control of law enforcement institutions. For example,

> as a decentralized digital currency system, *Bitcoin* lacks a centralized entity and is incapable of conducting due diligence (e.g., regulatory guidelines), monitoring and reporting suspicious activity, running an anti-money laundering compliance program, or accepting and processing legal requests like subpoenas (Federal Bureau of Investigation Report, 2012).

Secondly, virtual coins are based on cryptographic protocols and proof-of-work protocols (based on hashing algorithms) as security methods. Thereby, as explained above, "digital wallets" and digital currency transactions are safe, irreversible and do not contain personal information from the user. In addition to this feature, virtual money payments can be made without personal information being linked to the transaction - or, at least, apparently.

However, the blockchain technology used by the virtual coins requires that the transactions be exposed in a public register (for example, user A transfers a sum of 10 *bitcoins* to user B. Although the identities of the two are not known, the transaction itself is public, for an infinite term). Thus, all virtual currency transactions can be tracked and, finally, the IP addresses from which transactions have been made and associated with real identities can be found. This "impediment" can be solved too by using anonymization technologies such as *Tor* or *IpBouncing*, making it impossible to find the identity of the users.

Going further, an additional alternative - often used at the same time with Tor software, found by various users who want to keep their identity anonymity at all costs, is the use of a mechanism originally developed to offer intimacy and anonymity, called "mixers". These "mixers" are services that accept digital coins and return the same amount, minus a service charge, in the same virtual currency but the new coins are not associated with the original ones. Basically, the initial digital coins are mixed between as many users as possible. Most "mixers" work according to a privacy policy that specifies that transaction logs are removed after a short period of time, usually hours. For more certainty that identity can not be found, some users cross virtual coins through several types of "mixers".

Thirdly, international virtual money transfers have features that are not applicable to classical payment systems: they are almost instantaneous (there are rare cases where there is a wait time of up

to 30 minutes to confirm transactions), there are no commissions in the classical sense of the term for the transfer of the virtual currency (because, as we have seen, there are no "third parties" involved, the transfer is peer-to-peer, without intermediaries; yet a type of commission is practiced by the virtual currency system, but its value is reduced compared to the commissions for classic currency transfers - up to 0.2%, depending on the value of the transaction, and this commission is distributed to the network nodes and not to a distinct entity) and there is no maximum transfer limit or a limit over which transfers are controlled or examined by various institutions. Once transferred, virtual currencies can be exchanged in "classical" currency, such as euros or dollars, anywhere in the world, through "exchanges". Of course, some countries have a larger currency exchange system development for virtual coins (for example, Europe has clear advantages from this point of view towards certain countries in the Middle East, such as Syria or Iraq). So,

> the trading costs of digital coins are minimal, transactions are almost instantaneous and can be performed at any time. In addition, transactions should be immediate. No additional verification or validation should be required to execute any transaction. The person who sent the money should not be able to "unsend" it or reverse the transfer (Brill *et al*., 2014:14).

These general characteristics of *crypto-coins* make them attractive to terrorist groups. But, if we go deeper into this subject, we can see that among the over 700 different types of *crypto-coins*, some of them might be preferred to the detriment of others in illegal activities, due to their special features. Contrary to the fact that it is the first *crypto-coin* created, *Bitcoin* is not the first option when it comes to outlaw activities, including terrorist activities. The most eloquent examples in this regard are the *Monero* and *Zcash* coins. Unlike many *crypto-currencies* that are derivatives of *Bitcoin,* these two coins have different cryptographic algorithms that allow higher anonymity, making them more attractive to illegal activities. In both cases, payments are made public but the sender, recipient, and amount of the transaction remain private. Basically, the only information available on the blockchain will be the time on which transactions take place.

6. STATES' POSITION TOWARDS *CRYPTO-CURRENCY*

The feature of virtual coins to represent a decentralized payment form and therefore not to be created or controlled by any governmental institution (their issuance is not supervised by any central authority) and not to be regulated, has begun to raise numerous signals of alarm for institutions around the world lately, especially from the perspective of using virtual coins for illegal activities such as money laundering or terrorist financing. Gradually, various states have begun to take action on virtual coins. For example, Thailand was the first state in the world to ban the sale and purchase of *bitcoins* or products using this payment system. The decision was motivated by the fact that there are very few laws and capital controls in this area. Shortly after, in 2014, Russia also followed. The officials motivated their decision by the fact that the Russian legislation regulates the ruble as the only official currency and the introduction of any other coin or substitute is strictly forbidden.

Regarding the regulation and enactment of virtual coins, the first steps were taken by the FATF - the Financial Action Task Force, an intergovernmental organization founded in 1989 on the initiative of the G7 member states in order to create an "effective police body" able to fight against money laundering and terrorism financing.[1] The FATF recommendations establish a framework of measures that states should implement in order to combat money laundering and terrorist financing as well as financing the proliferation of mass destruction weapons. Taking into account the different legal, administrative and operational frameworks of the states, as well as different financial systems, FATF recommendations are a set of international standards that countries should apply by implementing measures tailored to specific circumstances. The FATF recommendations regarding terrorist financing set out the key measures that countries should take: risk identification, policy development and internal coordination; tracing money laundering, terrorist financing and funding the proliferation of mass destruction weapons; applying preventive measures for the financial sector and other designated sectors; establishing competences and responsibilities for competent authorities (e.g. investigation and law enforcement) and other institutional measures; promoting transparency and availability of information about the beneficiary; - facilitating international cooperation. (Financial Action Task Force, 2015). At European level, there are no official statistics on the issuance and use of virtual coins and it is intended to regulate virtual

[1] Fore more information about the Financial Action Task Force's activity: section *"Who we are",* FATF official website, available at http://www.fatf-gafi.org/about/

money for money laundering or terrorist financing by amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The European Central Bank (ECB) proposes to introduce virtual coins within the scope of the Directive. According to ECB, the virtual coins are defined as

> a digital representation of value not issued by a central bank or public authority, not linked to a fiduciary currency, has no legal status of currency or money but is accepted by natural or legal persons as a means of payment and can be electronically transferred, stored or traded (Voinea, 2017).

Thus, of interest for the *crypto-currency* area is the legislative package on money laundering prevention (replacing Directive 2005/60/EC, Directive 2006/70/EC and Regulation 1781/2006), which was adopted by the European Parliament on May 20th 2015 and published in the Official Journal of the European Union on June 5th 2015. The new legislation in the field strengthens E.U.'s restrictions in terms of preventing money laundering and ensures consistency with the international approach (Irimia, 2015). The EU legislative framework on money laundering prevention, adopted in May 2015, includes Directive (EU) No. 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and Regulation (EU) 2015/847 on information accompanying transfers of funds. Thus, Directive (EU) 2015/849 seeks to prevent the use of the EU financial system for the purpose of money laundering and terrorist financing. With regard to terrorist financing, the Directive defines this activity, through article 1 (5), Section 1, Chapter 1, as

> the provision or collection of funds by any means, directly or indirectly, with the intention of using them, or knowing that they will be used wholly or partly to commit any of the offenses within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA.

As mentioned above, at the level of the European Union, it is intended to amend this Directive in order to regulate virtual currencies.

5. CONCLUSIONS

The terrorist phenomenon has taken on a global dimension, especially in recent years, unimaginable at the start of the 21st century. The increasingly frequent and diversified attacks as well as the ingenious methods used by terrorist groups to reach their goals, whether we are talking about obtaining the weapons used in attacks or raising the funds needed to organize them, highlight the need to discourage and combat any form of support for the phenomenon since its incipient stages. The concept that *crypto-currencies* could be used to help fund terrorists has been a long-standing concern among law enforcement and government agencies worldwide. Indeed, many restrictions placed on the use of digital currencies stem from these concerns (Higgins, 2014). Indeed, due to their characteristics - decentralized payment form, based on cryptographic protocols, transactions are anonymous, they are obtained relatively easily by specific methods (mining) - virtual coins can represent a source of financing with a huge potential for development within the terrorist groups.

Although at this point in time the opinions about the use of virtual coins in the financing of terrorist activities are divided – there are voices who claim that it is impossible to put into practice this type of financing - yet the pace of development of the technologies involved and the basic characteristics of this type of currency urges the adoption of measures aimed at preventing the widespread of using *crypto-coins* among terrorist groups.

Among the recommended measures that may be taken by interested governments are: - stopping the anonymity of virtual currency transactions by imposing a traceability system which requires that these transfers of funds be accompanied by information about the payer and the payee; complying exactly with Directive (EU) 2015/849 according to which all Member States have set up or should set up autonomous and operationally independent financial intelligence units to collect and analyze the information received in order to establish links between suspicious transactions and underlying criminal activities to prevent and combat money laundering and terrorist financing; creating a virtual coin regulatory authority; - adopting legislation specific to the field of virtual coins and amending existing legislation in order to respond to the needs of this type of currency and to ease the efforts of the authorities in the fight against offenses related to them.

BIBLIOGRAPHY

1. Brill, A. E. & Keene, L. (May 2014) Cryptocurrencies: The Next Generation of Terrorist Financing? *Defence Against Terrorism Review,* Vol. 6, No. 1. [online]. Available: https://ssrn.com/abstract=2814914. [Accessed 03/05/2017].

2. Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis, OJ L 214, 4.8.2006. 29–34.
3. Directive (EU) 2015/849 Of The European Parliament And Of The Council Of 20 May 2015 On The Prevention Of The Use Of The Financial System For The Purposes Of Money Laundering Or Terrorist Financing, Amending Regulation (EU) No 648/2012 Of The European Parliament And Of The Council, And Repealing Directive 2005/60/EC Of The European Parliament And Of The Council And Commission Directive 2006/70/EC, OJ L 141, 5.6.2015. 73–117.
4. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005. 15–36.
5. Dumitru, B. (December 2017). Cum funcționează Bitcoin. *PressOne.* [online]. Available:https://pressone.ro/contributori/cum-functioneaza-bitcoin/. [Accessed: 02/05/2017].
6. European Central Bank. (February 2015). Virtual Currency Schemes – a further analysis. *European Central Bank official website*. [online]. Available: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf [Accessed: 04/20/2017].
7. European Central Bank. (October 2012). Virtual Currency Schemes . *European Central Bank official website*. [online]. Available: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. [Accessed: 04/20/2017].
8. European Commission. (February 2016). Communication From The Commission To The European Parliament And The Council On An Action Plan For Strengthening The Fight Against Terrorist Financing. *Eur-Lex*. [online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1455113825366&uri=CELEX:52016DC0050#document2. [Accessed: 04/20/2017].
9. Federal Bureau of Investigation. (April 2012). Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity Report. *Wired.* [online]. Available: https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf. [Accessed: 05/01/2017].
10. Financial Action Task Force. (2016). Consolidated FATF Strategy on Combatting Terrorist Financing. *FATF official website.* [online]. Available: http://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html. [Accessed: 04/27/2017].
11. Financial Action Task Force. (November 2015). Terrorist Financing - FATF Report to G20 Leaders – actions being taken by the FATF. *FATF official website.* [online]. Available: http://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-financing-actions-taken-by-FATF.pdf. [Accessed: 05/05/2017].
12. Higgins, S. (July 2014). ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide. *CoinDesk.* [online]. Available: http://www.coindesk.com/isis-bitcoin-donations-fund-jihadist-movements/. [Accessed: 05/05/2017].
13. Irimia, A.A. (October 2015). Directiva IV AML. Perspective de implementare. *Institutul Bancar Roman*. [online]. Available: http://www.ibr-rbi.ro/site/wp-content/uploads/2015/09/Anna-Angelica-Irimia.pdf. [Accessed 05/05/2017].
14. Martimof, B.M. (March 2010). Finanțarea terorismului. *Market Watch.* [online]. Available: http://www.marketwatch.ro/articol/5961/Finantarea_terorismului_(I)/.[Accessed 04/30/2017].
15. Mâță, D.C., (2016). *Securitatea Națională. Concept. Reglementare. Mijloace de Ocrotire.* Bucharest: Hamangiu.
16. Mitran, D. (May 2014). Istoria Bitcoin. *Bitcoin Romania*. [online]. Available: http://bitcoinromania.ro/blog/bitcoin/istoria-bitcoin/. [Accessed 30/04/2014].
17. Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds, OJ L 345, 8.12.2006. 1–9.
18. Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, OJ L 141, 5.6.2015. 1–18.
19. Voinea, O. (March 2017). Monede virtuale, tranzacții reale. *Revista Biz.* [online]. Available: http://www.revistabiz.ro/monede-virtuale-tranzactii-reale/. [Accessed 04/05/2017].