Blockchain Technology in Countering Cyber Threats

Elena Aleksandrovna Antonyan[1*], *Natalya Aleksandrovna* Grishko[2], and *Marina Mikhailovna* Milovanova[1]

[1]Kutafin Moscow State Law University, Department of Criminology and Criminal and Penal Law, Moscow, Russia

[2]Ryazan State University named for S. Yesenin, Department of theory of Law and administrative legal disciplines, Ryazan, Russia

Abstract. The prerequisites for the study are the widespread use of blockchain technology in various sectors of human life support where its application is an opportunity to repel cyber threats the forms of manifestation of which will only increase in the age of new technologies. The spread of cyber threats necessitates a set of measures aimed not only at identifying and combating them but also at active working to prevent their spread. The study aims to comprehensively study the use of blockchain technology in countering cyber threats. The research methods are as follows: a reasonable combination of the general scientific dialectical method with legal positivism; social relations and phenomena and their interaction with scientific categories in dialectical unity; consideration of a separate process based on comparative legal positivism; scientific methods of analysis and synthesis, induction and deduction. Results and novelty: today the creation and functioning of security systems, given the multiple nature of the factors of influence on electronic and telecommunication systems, should be complex; local attempts to counter cybercrime give short-term and ineffective results. Arguments are presented for the fact that today blockchain technology is one of the most modern means of countering cybercrime. This is due to the fact that it has a significant period of operation which allows conclusions to be drawn about its functionality and effectiveness, the availability of proven material and technical means and technologies for its implementation in the social sphere, as well as the possibility of its further development and improvement in relation to countering cyber threats in the conditions and vulnerabilities of the blockchain.

Keywords: terrorism, Internet, technology, crime prevention

1 Introduction

Over the past three decades, the global electronic and telecommunications system (let us call it the Internet) has worked its way from primitive to high-tech and has undergone major

[*] Corresponding author: antonyaa@yandex.ru

changes. A significant breakthrough has been made in technological terms, which has made it possible to significantly increase the effectiveness of its use in almost all spheres of the functioning of modern society. Moreover, alternative systems and technologies have begun to appear and are now actively used, operating alongside official, publicly available systems. This situation is inevitable, given the nature of its functioning and the legal order of regulation of the industry in question. On the one hand, there is an active introduction of the achievements of scientific and technological progress to increase the efficiency of the operability of electronic and telecommunication systems on a global scale. On the other hand, it would be absurd to assume that such technologies have been deprived of the attention of illegal (criminal) structures of various levels.

The development of criminal activity in the field of cyber threats is carried out in three main directions: only for deriving profit; the possibility of political influence on the official authorities, in this case, we are talking about active manifestations of cyber terrorism and cyber extremism; and mixed. This situation, in our opinion, is due to a number of interdependent factors the list of which presented is not exhaustive:

First, at the initial stage of development of electronic and telecommunication systems, the necessary condition for the creation and development of technologies for their protection was not taken into account since their possible use for criminal and other illegal purposes was not assumed;

Secondly, over time, electronic and telecommunication systems and networks began to be actively used to apply new forms of influence (cyber weapons) which required the creation of alternative technologies and networks that was originally carried out by special state units (special services), and they were supposed to be used along with official systems and technologies, to increase the level of secrecy for subsequent use on electronic and telecommunication systems in relation to the countries considered as enemies. This is how DarkNet appeared (a private network, the essence of which is interconnection only with trusted persons. The Darknet's extremist nature is quite clearly manifested, since along with criminal manifestations of the general criminal direction, aggressive organizations are actively discussing terrorist activities, their propaganda, involving recruits, as well as methods and options for unblocking politically undesirable sites, etc.). Today, there are already quite a large number of such systems and networks (Surface Web, Deep Web, 12P, Freenet, etc.) and most likely their creation will not be limited to this.

Thirdly, as a natural development of the technologies under consideration, participants in criminal and active radical organizations gained access to these developments and began to actively use them for criminal purposes.

Fourthly, taking into account the system of organization and functioning of criminal structures, they create the most favourable conditions for further adaptation, improvement and use of the received electronic software elements for criminal purposes much faster and more efficiently.

Aim of the study. The study shows that in different periods of time there is a simultaneous and interdependent development of technologies of electronic and telecommunication systems in the legal field and the criminal part. The achievements of scientific and technological progress in the field of electronic and telecommunication technologies and systems are being actively adopted by aggressive and criminal structures.

2 Methods

Comparative and legal, historical, structural and logical methods form the basis of the given study.

3 Results

The factor is the untimely and sometimes inadequate reaction of countries to cybercriminal manifestations, especially in those cases when they do not affect the interests of a particular country. And only in the event of an impact on the electronic and telecommunication systems of a given country, it begins to show interest in the emerging problem.

As a technical factor, imperfection of the material and technical support of electronic and telecommunication systems affects the possibility of a criminal impact on the considered elements. According to various data from various sources, today the most popular operating systems have about a hundred or more vulnerabilities.

In addition to all of the above, at all times, one of the factors seriously affecting the safety of electronic and telecommunication systems remains the human factor (cyber hygiene). According to the research of specialists and scientists, a significant number of the personnel using external and internal information networks in their activities quite often open attachments coming to their computer, thereby allowing criminals access to the networks and computer hardware of their enterprises, institutions and organizations, since a significant number of these attachments, as a rule, contain a virus and they are sent with the aim of a certain impact on the addressee’s computer.

Taking the current situation into consideration, today's creation and operation of security systems, given the multiple nature of the factors of influence on electronic and telecommunication systems should be complex. Local attempts to counter cybercrime give short-term and ineffective results. For example, to counter cybercrime, measures are now being taken to identify both infected and infecting systems, which, according to most scientists, is currently an ineffective means of countering cybercrime [1]. This is due to the nature of the generalized statistical material of the development of cyberspace in the third decade of the 21st century [1].

4 Discussion

In this regard, on the one hand, one should partially agree with the opinion of scientists, “that the main measure of countering cybercrime at the state level is precisely legal regulation, that is improving legislation, criminalizing new acts, toughening responsibility for already existing crimes in the sphere of cyberspace [2].

On the other hand, according to scientists and experts, an integrated approach is needed, the essence of which is that “the main measures include the adoption of laws, strategies to counter cybercrime, effective leadership, capacity development of criminal justice and law enforcement agencies, educational outreach activity, building a solid knowledge base, and collaboration between government and the private sector. Certainly, an important factor is a proper attitude to the computer information which is of certain interest to another subject and restricting access to such information by using licensed computer programmes and antivirus software to protect the computer from illegal hacking [3].

Given the nature of the modern development of society, a paradoxical situation is emerging. The existence and further development of parallel electronic and telecommunication networks which has received the name of the “deep network” (“dark Internet”, etc.), is recognized as quite harmful and unsafe for the existence and functioning of generally recognized electronic and telecommunication networks, and as a result, harmful to the geopolitical structure of the world. However, for example, the TOR Browser system application (The Onion Router) used to connect to the “deep network”, is now being developed and improved by the completely legal and well-known TOR Project Company, and the browser is open access and freely available. In addition, today a more advanced version of Tor2Web is already available which uses the Botnet malicious system, and proxy servers are already used to implement the activities of the Bots. As the name implies, the Tor network is used for the functioning of the entire system in which blockchain technologies are actively used to protect it.

The entire system of the “deep network” functioning is built on the principle of an onion (onion head) which lies in the fact that any message is “wrapped” in several layers of encryption, and only after that, it becomes possible to transmit it through a large number of network nodes called onion routers. In the process of transmission, each node removes the protective layer to establish each subsequent node in this chain, and the final result, that is, complete decryption, is carried out only by a specific recipient. This process provides anonymity, since no intermediary can see either the contents of the message being forwarded or the route it was forwarded.

It becomes clear that blockchain technologies are used to protect the “deep network”, the characteristic feature of which is a diametrically opposite principle of operation. In general, its appearance goes back to the 90s of the last century. Within the framework of our research, this is the background information which is still being discussed. However, it seems interesting to us that blockchain technology appeared precisely in the vastness of the “deep network”.

Thus, it took a significant period of time for scientists and specialists from various industries to speak about the blockchain, its development and implementation in electronic and telecommunication systems as a revolutionary phenomenon.

The principle of the blockchain is that it is a P2P distribution (peer to peer-computer network where all participants are equal), and it is a ledger system where everyone can see how the other user enters but nothing can be changed. Thus, blockchain is a distributed peer-to-peer ledger that is secure and used to record transactions across many computers. The content of the ledger can only be updated by adding another block related to the previous block. It can also be thought of as a peer-to-peer network running over the Internet.

In amateur’s or business’s terms, blockchain is a platform where people are allowed to conduct any kind of transaction without the need for a central or trusted arbiter. The created database is shared among network participants in a transparent way so that everyone can access its contents. The database is managed autonomously using peer-to-peer networks and a timestamp server. Each block in the blockchain is organized in such a way that it refers to the content of the previous block. The blocks that make up the blockchain contain batch transactions approved by the network participants. Each block comes with a cryptographic hash of the previous block in the chain [4].

As mentioned earlier, the block building system in the blockchain is the opposite of the TOR system which, on the contrary, allows you to track all participants, as well as the path of a message or transaction. Taking into account the fact that these two technologies are combined plus the use of the capabilities of the Botnet malicious system which already uses the capabilities of proxy servers, it becomes clear that cybercriminals are not twiddling their thumbs and are actively developing their systems to overcome security systems. The current situation requires the adoption of timely and adequate measures aimed at combating cybercrime.

Recent studies in this area show that today blockchain technology is one of the most modern means of countering cybercrime. This is also due to the fact that it has a significant period of time of operation which allows conclusions to be drawn about its functionality and efficiency, the availability of proven material and technical means and technologies for its implementation in the social sphere, as well as the possibility of its further development and improvement.

However, we have to talk about the problems of blockchain vulnerability as well. Firstly, today this technology is not fully ready for increasing the number of users (scaling). This is due to the power of computer hardware which is not able to process a colossal amount of information when building blocks.

Secondly, the blockchain has an element of publicity, which also negatively affects the process of its implementation. Individual users are not ready to advertise their transactions which sometimes have elements of a criminal nature, which attracts them to use the capabilities of the "deep network".

Thirdly, as is often the case, the lack of potential knowledge about the functioning structure and system of the technology among a wide mass of users, which significantly slows down the process of its implementation in the electronic and telecommunication systems of society and the state. However, for some time now there has been talking about the possibilities of creating a public blockchain which will be available to all users of the open network, the Internet.

So, in 2013, experts started talking about a new solution to the problem and the development of a decentralized software platform built on the basis of the blockchain. This solution is called Ethereum. This platform allows anyone using their computer to create new blockchain services or applications. Ethereum provides many opportunities for people through its implementation in various areas of life:

- creation of financial contracts;
- implementation of crowdfunding and investment projects;
- insurance activities and so on.

At the moment, the development of Ethereum technology is also continuing. Based on this platform, several dozens of new cryptocurrencies have already been created and hundreds of services and applications have been launched [5].

Given the current situation, experts are already informing about the large-scale development of blockchain technologies at various levels, which has led to the emergence of such technologies as private, hybrid and federated blockchains. This view is shared by most cybersecurity organizations, as evidenced by the statistics presented in their online fraud reports [6-8].

This situation, in full measure, allows us to talk about the promising possibilities of using blockchain to combat cybercrime in general, both in relation to individual citizens and to protect the most vulnerable government and other institutions from cyber threats including cyber terrorism and cyber extremism. The term cyber terrorism itself "has the same degree of clarity as the term cybersecurity, that is, it does not have it at all" [9].

However, it would be wrong to speak out about the exceptional possibilities of building security only on blockchain technology. It seems that today we should talk about the development of comprehensive measures to protect the electronic and information environment based on other technologies, such as additive technologies, big data technologies, technologies of the General Internet the Internet of Everything), the Internet of Things, virtual reality technologies (virtual reality, VR, artificial reality), artificial intelligence technologies, and others [10].

Some of them are already beginning to be implemented in our state. So, at present, Russia has adopted the Law on an experimental legal regime for the introduction of artificial intelligence technologies in Moscow. The law provides for an experiment in Moscow to establish a special legal regime from July 1, 2020 "in order to create the necessary conditions for the development and implementation of artificial intelligence technologies, as well as the subsequent use of the results of its application". The conditions, requirements, the procedure for the development, creation, implementation and realization of artificial intelligence technologies, as well as the mechanism for processing anonymised personal data will be regulated by the Moscow Government. The purpose of the experiment is to radically simplify the conditions for companies developing artificial intelligence and establish clear-cut and easy-to-understand rules for the development of technologies based on it. Artificial intelligence easily works with huge amounts of data including helping to make decisions and freeing people from routine tasks. At the same time, many aspects of the use of technology today are not legally regulated.

Given that artificial intelligence is capable of self-learning and does it faster than humans, the speed of emergence of new digital solutions will only increase [11]. The strategies and tactics of modern terrorist organizations have a technological focus [12].

However, with the introduction of these technologies, certain difficulties may arise. As noted in most sources, this is because Russia does not have its own production of material, technical and software for electronic and telecommunication systems, which entails the need to use foreign products, and this can have negative consequences, since they may initially have hidden threats to influence safety our state.

In addition, it should be noted that at present in this area there is a shortage of highly intelligent personnel who can implement the developed programmes at a high professional level, which will require their timely and high-quality training.

5 Conclusion

The entire mechanism for the implementation and functioning of state programmes also requires high-quality protection, which in turn necessitates modern high-quality training of law enforcement officers in the field of information security capable of resisting cyber threats, their constant training and internship.

In addition, the possibilities of increasing the level of cyber hygiene, as well as countering cyber terrorism and cyber extremism, should be carried out at the earliest stages of education, especially in the general educational environment. It is argued that cyber terrorism forms the rapprochement of two worlds – virtual and physical [13]. Today, there are no regulations that would reflect the problems of cybercrime in general, cyber terrorism and cyber extremism [14].

So, according to scientists, the prevention of cyber extremism among young people should be carried out simultaneously in three areas: legal, acmeological and technological [15].

The study was carried out with the financial support of the Russian Foundation for Basic Research within the framework of Blockchain Technologies for Countering the Risks of Cyber terrorism and Cyber Extremism scientific Project No. 18-29-16175: a Criminal-Legal Study.

References

1. A.P. Sukhodolov et al. Rus. J. of Crim. **13(4)**, 558-559 (2019)
2. E.A. Antonyan and E.V. Barkhatova, Eura. Union of Sci. **7(64)**, 55 (2019)
3. L. Gubanova, 2019 – God federativnogo blokcheina – konsortsiumnogo blokcheina. Prostoe obyasnenie [2019 – The Year of Federated Blockchain, Blockchain Consortium. Simple explanation]. Accessed on: April 09, 2021. [Online]. Available: https://clck.ru/UCo7c
4. D. Makarenko, Istoriya razvitiya i budushchee tekhnologii blokchein [Development History and Future of Bblockchain Technology]. Accessed on: April 09, 2021. [Online]. Available: https://masterlan.info/flf/kriptovalyuta/kto-pridumal-blokchejn.html
5. Internet Security Threat Report **24** (2019). Accessed on: April 09, 2021. [Online]. Available: https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf

6. Norton Cyber Security Insights Report 2017 Global Results (2017). Accessed on: April 09, 2021. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf
7. PwC 2018 Global Economic Crime and Fraud Survey (2018). Accessed on: April 09, 2021. [Online]. Available: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf
8. ThreatMetrix A LexisNexis Risk Solutions Company. Q1 2018 Cybercrime Report (2018). Accessed on: April 09, 2021. [Online]. Available: https://www.threatmetrix.com/digital-identity-insight/cybercrime-report/q1-2018-cybercrime-report/
9. Peter W. Singer. The Cyber Terror Bogeyman (2012). Accessed on: April 09, 2021. [Online]. Available: https://www.brookings.edu/articles/the-cyber-terror-bogeyman/
10. N.G. Zhavoronkova and Yu.G. Shpakovsky, Legal Sci. without Bord. **3**, 165 (2020)
11. Federalnyi zakon ot 24.04.2020 № 123-FZ «O provedenii eksperimenta po ustanovleniyu spetsialnogo regulirovaniya v tselyakh sozdaniya neobkhodimykh uslovii dlya razrabotki i vnedreniya tekhnologii iskusstvennogo intellekta v subekte Rossiiskoi Federatsii – gorode federalnogo znacheniya Moskve i vnesenii izmenenii v stati 6 i 10 Federalnogo zakona «O personalnykh dannykh» [Federal Law of 24.04.2020 No. 123-FZ On Conducting an Experiment to Establish Special Regulation in order to Create the Necessary Conditions for the Development and Implementation of Artificial Intelligence Technologies in the Constituent Entity of the Russian Federation – the Federal Significance City of Moscow and Amending Articles 6 and 10 of the Federal Law About Personal Data]. Accessed on: April 09, 2021. [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_351127/
12. M. Zerzri, The Threat of Cyber Terrorism and Recommendations for Countermeasures. C·A·Perspectives on Tunisia No. 04- Accessed on: April 09, 2021. [Online]. Available: https://euagenda.eu/upload/publications/untitled-145478-ea.pdf
13. E.A. Antonyan and N.A. Grishko, New Technologies in Cyber Terrorism Countering in Proc. XVII Int. Research-to-Practice Conf. (March 2020). https://doi.org/10.2991/assehr.k.200321.078
14. B. Colin, Crime and Justice Int. **13(2)**, 15-18 (1997)
15. V.N. Makashova, Fundamental Research **10(9)**, 2055 (2013)