New Technologies in Cyber Terrorism Countering

Antonyan E.A.[1,*] Grishko N.A.[2]

[1]*Moscow State Legal University named after O.E. Kutafin, Russian Federation, Moscow*
[2]*Ryazan State Agrotechnological University named after P.A. Kostychev, Russian Federation, Moscow*
[*]*Corresponding author. Email*: antonyaa@yandex.ru

ABSTRACT

The article considers new technologies for cyber terrorism countering. Cyber terrorism is aimed at destabilizing public order, large-scale disruption of communication systems, intimidation by imposing one's will, including on authorities, and, in general, it is an increased threat to the state's national and information security. Particular attention is paid to blockchain technology, which allows hiding funds aimed at financing terrorist activities, including in the information space. The article provides the generalized results of a study in the framework of the implementation of the Russian Foundation for Basic Research scientific project No. 18-29-16175 "Blockchain technology to counter the risks of cyber terrorism and cyber extremism: criminological and legal research". To date, there are no internationally normative legal acts that would reflect the problem of cybercrime in general, cyber terrorism and cyber extremism in particular. International legal acts should provide comprehensive and effective measures to counter such crimes, which must be implemented in the national legislation of various states, including international cooperation

Keywords: *law enforcement, new technologies, counteraction, cyber terrorism, information security, increased threat*

1. INTRODUCTION

In the modern period, a general system of normative legal acts has been formed in the field of countering cyber extremism and cyber terrorism.

First of all, the importance of the UN fundamental documents, that define the basis for cooperation in the field of crime prevention in general, should be noted. At the same time, it is important to underline that "the UN has been actively involved in the development and dissemination of internationally recognized principles in the field of crime prevention and criminal justice since its foundation".

The documents defining the main provisions (principles) of crime prevention and international cooperation: UN Declaration on Crime and Public Security (General Assembly resolution 51/60 of December 12, 1996); Vienna Declaration on Crime and Justice: responses to the challenges of the 21st century (UN General Assembly resolution 55/59 of December 4, 2000; Guidelines for the prevention of crime (Economic and Social Council resolution 2002/13 of July 24, 2002); Bangkok Declaration on Interaction and Response: strategic alliances in the field of crime prevention and criminal justice (UN General Assembly resolution 60/177 of December 16, 2005); Salvadoran Declaration on Integrated Strategies for Responding to Global Challenges: crime prevention and criminal justice system and their development in a changing world (UN General Assembly resolution 62/230 of December 21, 2010), etc. In general, many issues related to the threat of cybercrime are discussing at various UN events. So, this Organization has been considering various processes in the areas related to the use of computers starting from the XIII UN Congress on the Prevention of Crime and the Treatment of Offenders in 1990, but so far the UN has not developed and adopted a document that would be devoted specifically to counteracting cybercrime in modern conditions, i.e. would meet the needs of modern society and the new challenges of crime.

The Council of Europe, as an authoritative international regional Organization, has also adopted a number of documents establishing fundamental provisions in the fight against crime, the most important of which is the Computer Crime Convention (Budapest, 2001), which emphasizes the importance of strengthening cooperation between states aimed at protecting society from crime in the field of computer information.

2. RESEARCH METHODOLOGY

Obviously, the legal basis taking into account modern realities, global threats to the world community, which are cybercrime, cyber terrorism, and cyber extremism, should be developed on the international level.

3. RESULTS

A number of regulatory legal acts have been adopted and are in force in the Russian Federation. However, there is no specific regulatory act dedicated to combating

Copyright © 2020 The Authors. Published by Atlantis Press SARL.
This is an open access article distributed under the CC BY-NC 4.0 license -http://creativecommons.org/licenses/by-nc/4.0/.

cybercrime, cyber terrorism and cyber extremism in the Russian state. So far, a unified approach to the definition of these negative social phenomena at the legislative level has not been developed.

In recent years, the processes of digitalization and globalization taking place in the world have enabled almost every person to take advantage of the modern world’s innovative phenomena. This greatly facilitated the interaction of people in society, but at the same time, modern technological achievements of mankind are also used to violate the law, creating new technologies for criminal activity in the world. Reliance on the advantages of information and digital technologies, as the main sign of new forms of criminal acts, naturally required new forms of counteraction from the national security systems of the countries of the world.

One of these threats of a completely new type is, for example, the use of cryptocurrency in order to finance terrorist and extremist organizations. Cryptocurrency is a fully virtual currency unit that does not have physical equivalents and is implemented today in the form of "bitcoin". Bitcoin is completely independent of states and banking systems. A special element of this payment system is the basic client program. Client programs launched on many computers are connected to each other in a peer-to-peer network and no one can arrest it even temporarily, and it is extremely difficult to track financial transactions. At the same time, sending bitcoin from one wallet to another is completely anonymous. Not surprisingly, this technology is the base of the modern economy of banned organizations.

The most important aspect of new forms of combating crime is the deanonymization of anonymous proxy server systems users. And if earlier the security agencies still had accessible "loopholes" for direct access to the user's IP address, now everything has become much more complicated and comprehensive analysis of the traffic of a particular user is needed.

In the Russian Federation, SORM-3 is used as the main tool for combating such forms of crime. This system provides control of some VPN servers, wiretaps in real time satellite communications, instant messengers, stores metadata about calls, Internet sessions, and allows receiving data from the operator’s internal systems.

This technology is almost guaranteed to stop any attempt at terrorist activity. And if in the conditions of a developed Internet, security agencies might have problems encrypting messages between criminals through a virtual private network (VPN), then this system solves this problem. The ability to monitor instant messengers such as Telegram, of course, is the key value of this unique system, since it is precisely them that terrorists and extremists use for communication.

4. DISCUSSION OF THE RESEARCH RESULTS

In the Russian Federation, crimes are increasingly committed using technology, and this requires a special response from state security. However, the practice of using our SORM-3 system as a new form of combating crime is minimal. The technological potential of the security agencies of the Russian Federation is undoubtedly high, but it is insufficient for the targeted suppression of particularly technologically sophisticated criminal acts related to cryptocurrencies and anonymous proxy servers. Since there are difficulties with state control of the blockchain cryptocurrency, in order to protect the country from the financial gain of prohibited organizations, it is necessary to determine cryptocurrency (bitcoin) as a crime. Other measures aimed at developing new forms of combating crime are impossible without a joint law enforcement reaction to the international crime network (drug trafficking, crypto financing of banned organizations) under the collective security treaty of the CIS member countries. It can be stated that, given the technological development of our countries, joint efforts would guarantee a powerful blow to crime.

Blockchain is a technology that has a chance to turn the sphere of state regulation, the sphere of the state as a whole, and also all spheres of finance. Fields of application of such technology are multiplying every day: there are more and more areas in which blockchain can play the role of a modernizing element. Among them is criminology, and blockchain has to form links with it.

Blockchain is a continuous sequential chain of blocks containing information. Each block has metadata in its heading (for example, a unique checksum, creation time), as well as a link to the previous block. The content of the block is usually a list of digital assets and teams like completed transactions, their volumes and addresses of participants in transactions. The chain forms a decentralized database, which is a distributed journal for recording operations.

The information contained in the blocks of the chain can be obtained by all users of the network who have access to it. Access is opened by a special private key created on the basis of a cryptographic algorithm. Thus, the storage and transmission of data in the blockchain chain is protected and secure.

The database saves the entire history of transactions committed within the chain. Information about them is available to all users and can be checked at any time. When a new data block is formed, the registry is updated simultaneously on all computers on the network. After the appearance of a new block, it is impossible to change its data, which means it is impossible to fake. Thanks to these features, the system is transparent and reliable.

Initially, it was assumed that blockchain technology guarantees complete freedom and independence of the chain, the absence of a single administrator, that is, the absolute decentralization of internal processes. However, due to the interest in the new technology of large companies and financial institutions, other forms of blockchain appeared, more centralized and controlled. They differ in the level of access to information of blockchain network participants, as well as their ability to influence its development.

There are a public blockchain; consortium blockchain; private (fully private) blockchain.

In the public blockchain, transactions are carried out freely and are not controlled by anyone. Anyone can access it. The processes occurring in the system are watched by all network participants, from developers to service providers and ordinary users. Everyone has the opportunity to send transactions, take part in the consensus process and determine which blocks will be added to the network and which ones will be rejected.

Public blockchains are protected by the principles of cryptoeconomics, which is based on a combination of economic incentives and cryptographic computing. This is the main difference between open blockchains and ordinary economic systems, which are strictly regulated and managed centrally. At some points, even the creators of the system cannot influence it in any way and make any corrections to the code or data. The system is protected from developer intervention, as well as from hacking. Maintaining security does not require a large amount of funds, but its weakening may require considerable computing power, which makes the attack disadvantageous for attackers.

The activities of consortium blockchains are controlled by a pre-selected set of nodes. So, some blocks must recognize others as valid for adding the latter to the chain. For example, tracking the transportation of goods uses such an algorithm. The blockchain can be either publicly available or visible exclusively to participants in the blockchain network. There are also "hybrid" systems in which root blocks are publicly available, but all members of the blockchain can make only a limited number of requests and confirmations of transactions of some parts of the blockchain.

A private (fully private) blockchain is a chain of blocks in which the addition of new blocks is carried out by one organization. Access to block information can be open or limited to one degree or another. Such a system is completely centralized; therefore, in terms of access level, it is close to classical networks.

The advantages of private blockchains are validators that protect the system from attacks with high speed of transaction confirmation, the ability to control the network with a single center. Thus, it is possible to quickly update and improve the functionality of the system, more accurately predict further actions and make the necessary changes to the blocks.

Initially, blockchain began to be used on the cryptocurrency market. It was seen as an alternative to the existing banking system. However, it was banks and other financial institutions that subsequently showed great interest in blockchain technology, since it has the properties necessary for storing and protecting information. Thanks to it, participation in transactions of third parties is excluded, the foundations of the economy of robots are laid.

At the moment, representatives of dozens of different fields are interested in technology. Some countries plan to maintain a land registry with its help, combating land fraud. Digital identity cards, systems for confirming and maintaining copyright and authenticity are created on the basis of the blockchain. The diamond and energy industries are working on introducing this technology to solve problems in the field of production and consumption of resources. Electronic platforms for anonymous online voting on the basis of the blockchain are actively developed. It also found its application in the fields of video games, business, private and public administration.

The possibilities of such an application are endless thanks to such blockchain properties as general accessibility, reliability, high adaptability and profitability. Thus, it is possible to combat cyber terrorism, cyber extremism and other types of crimes on the Internet. However, it is important to note that the illiterate disposition of blockchain from the technical side can lead to the risk of increased criminal activity and cyberattacks, since thanks to the development of digital technologies, cyber terrorists have more opportunities for more sophisticated crime planning.

Blockchain technology is guaranteed to protect the system from fakes and fraud, this prevents terrorists and extremists from quickly and anonymously attacking and getting the information they need. The blockchain can become the basis of cybersecurity in the event that user data is stored on its network. It protects data from hacking, theft or destruction of information. When a traditional system is hacked, a hacker can gain access to thousands of objects, but when a blockchain system is hacked, he will have access to only one block of information. This complicates the work of the criminal, since he will have to decipher each fragment individually to get all the information. Anti-terrorist groups in some countries are already using supercomputers with advanced software, in particular blockchain technology, to calculate the likelihood of cyberattacks, to collect and analyze large amounts of data from the Internet, to identify and recognize the location, movement and interpersonal relationships of cyber terrorists, as well as to identify suspected individuals and control over their criminal activity.

In this regard, there are trends towards the development and improvement of legislation in the information sphere. So, at the beginning of 2018, the law "On the security of critical infrastructure" came into force in Russia. This document explains which government agencies and companies should consider themselves critical and in what ways data can be protected. It is worth noting that responsible organizations must also report incidents and undergo a safety assessment. Also, a document came into force that allows protecting the financial resources of citizens and organizations. In May 2018, the Bank of Russia amended the regulation "On requirements for ensuring the protection of information". In February 2019, in Clause 1 of the Resolution of Plenum of the Supreme

Court of the Russian Federation "On judicial practice in cases on legalization (laundering) of money or other property obtained by criminal means and on the acquisition or sale of property knowingly obtained by criminal means" was amended, according to these amendments the subjects of the crimes provided by articles 174 and 174.1 of the criminal code may include funds converted from the virtual assets (cryptocurrencies) acquired as a result of the crime. Thus, the Supreme Court of the Russian Federation equates cryptocurrency with property.

5. CONCLUSION

Today, first of all, at the international level, there are no normative legal acts that would reflect the problem of cybercrime in general, cyber terrorism and cyber extremism in particular. International legal acts should provide comprehensive and effective measures to counter such crimes, which must be implemented in the national legislation of various states, including international cooperation.

In addition, a unified approach to understanding the terms "cyber terrorism" and "cyber extremism" has not been formed in Russian legislation, which leads to inconsistency in the provisions of various regulatory legal acts and an unclear definition of the competence of law enforcement agencies in combating these negative social phenomena.

REFERENCES

[1] E.A. Antonyan, I.I. Aminov. Blockchain technology in countering cyber terrorism // Actual problems of Russian law, No. 6 (103), 2019. - 167 - 177.

[2] Baulin. Cryptocurrency has come under control: ICO banned in China // URL: https://www.forbes.ru/tehnologii/349825-kriptovalyuta-popala-pod-kontrol-v-kitae-zapretili-ico. - date of the application: 04/20/2019.

[3] S. Nakamoto. Bitcoin: digital peer-to-peer cash system // URL: http://bitcoinwhitepapers.com/bitcoin_ru.pdf. - date of the application: 12/20/2019.

[4] Yu. Sergeeva. Internet 2017-2018 in the world and in Russia: statistics and trends // URL: https://www.web-canape.ru/business/internet-2017-2018-v-mire-iv-rossii-statistika-i-trendy/. - appeal date 04/20/2019.

[5] V. Smerkis. Experience of developed countries: why the EU has banned anonymous cryptocurrency trading // URL: https://www.forbes.ru/tehnologii/360519-opyt-razvityh-stran-pochemu-es-zapretil-anonimnuyu-torgovlyu-kriptovalyutami - appeal date: 04/20/2019.

[6] A. Bourue How Blockchain Can End Cannabis Looping And Smurfing Schemes // URL: https://www.forbes.com/sites/andrebourque/2019/02/28/how-blockchain-can-end-cannabis-looping-and-smurfing-schemes/#56db5aa2605f. - appeal date 04/20/2019.

[7] A.P. Sukhodolov, E.A. Antonyan, M.V. Rukinov, M.Yu. Shamrin, M.G. Spasennikova. Blockchain in digital criminology: statement of the problem // All-Russian Criminological Journal. 2019. V. 13, No. 4. P. 555-563.

[8] Tokes Platform Whitepaper // URL: https://tokesplatform.org/ - date of contact: 04/20/2019.

[9] D. Volodzko. Japan's Cyber terrorism Crisis Threatens Us All // URL: https://www.forbes.com/sites/davidvolodzko/2018/11/26/japans-cyberterrorism-crisis-threatens-us-all/#30c943846878/ - Date of access: 03/18/2019.

[10] M. Zerzri. The Threat of Cyber Terrorism and Recommendations for Countermeasures. C·A·Perspectives on Tunisia No. 04-2017 | cap-lmu.de. Zerzri - Cyber Terrorism. // URL: https://www.cap-lmu.de/download/2017/CAPerspectives-Tunisia-2017-04.pdf. - appeal date 03/18/2019.