DOCTRINAL COMPREHENSION OF CYBER TERRORISM IN THE CONTEXT OF INTENSIVE DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE MODERN WORLD *

AUTHORSHIP

Dmitry V. Lobach

Candidate of Legal Sciences, Associated Professor, Department of Theory and History of Russian and Foreign Law, Institute of Law, Vladivostok State University of Economics and Service, Vladivostok, Russia.

ORCID: https://orcid.org/0000-0002-7229-439X
E-mail: dimaved85@mail.ru

Alexey Y. Mamychev

Doctor habil. in political science, Phd in legal science, head of the laboratory of political and legal research, Lomonosov Moscow State University, Professor of Vladivostok State University of Economics and Service.

ORCID: https://orcid.org/0000-0001-6528-2836
E-mail: mamychev@yandex.ru

Olga I. Miroshnichenko

School of Law, Far Eastern Federal University, Vladivostok, Russia, Ph.D. in Law, Ll.M. In legal theory, Associate Professor of the Department of theory and history of state and law, Russia, Vladivostok, 8 Sukhanova Street.

ORCID: https://orcid.org/0000-0003-0135-3855
E-mail: olga-star.05@mail.ru

Lidiia Moskvych

Doctor of Law, Yaroslav Mudryi National Law University (61024, Ukraine, Kharkiv, Pushkinskaya str., 77.

ORCID: https://orcid.org/0000-0001-7339-3982
E-mail: moskvichlida@gmail.com

Received in:	**Approved in:**
2020-01-10	2020-01-29

DOI: https://doi.org/10.24115/S2446-6220202172702p.201-208

INTRODUCTION

The intensive development and widespread dissemination of information and communication technologies (hereinafter referred to as ICT) in the modern world aggravated by the complication of social relations in the direction of political and economic unification and diversification determine the modernization of society, which is manifested in the digitalization of social relations and management processes, as well as in the creation of a single information space on the basis of the Internet network.

At the same time, the globalization of the economy, accompanied by an exponential growth in the introduction of new telecommunication technologies and an active digital transformation of various spheres of society (for example, communications, transport, medicine, education, energy, financial system, state and municipal administration, defense and national security) increasingly predetermines the spread of terrorist acts using high technologies in the information space. In this context, special attention should be drawn to such destructive use of ICTs to undermine public order, destabilize the work of government bodies and Academic interest in cyber terrorism is dictated by the special nature of the public threat of terrorism in general, which is expressed in an encroachment on state security, public order and civil peace.

Subject to the global processes of informatization, computerization and digitalization that are available in the systems of public administration, production, distribution of material benefits and covering practically all spheres of society, it is natural to assume about the likely threats to public order and private interests emanating from unlawful acts in cyberspace inspired by terrorist organizations. In this vein, special attention in the special literature is paid to increasing the information and technological potential of terrorist organizations (ASHRAF & FILIPPIDOU), which predetermines new threats to the economic stability of individual states, since disruptive (breakthrough) technologies used in cyberspace for criminal purposes can cause enormous material damage (both direct and indirect) to critical infrastructure facilities (for example, water supply, electricity, healthcare, telecommunications).

For example, economic calculations related to the damage and costs that may arise because of cyberattacks on critical infrastructure facilities show that soon cyberattacks can lead to losses of up to $ 3 trillion, while recovery work carried out after committing cybercrimes are estimated at between $ 375 billion and $ 575 billion a year. According to the Lloyd's Centre for Risk Research and Cambridge University, a power outage due to a cyberattack on US power grids will cost the State $ 243 billion to $ 1 trillion and will also have a significant impact on mortality.

*The study was carried out with the financial support of the Russian Foundation for Basic Research within the framework of scientific project n. 20-511-00009.

In turn, the Centre for Strategic and International Studies estimated the probable annual costs of restoring and repairing systems damaged by cyberattacks and losses from economic espionage in the global economy at more than $ 445 billion (AKHGAR & BREWSTER, 2016). At the same time, despite the academic updating, wide media coverage and political speculation about this phenomenon, there is still the problem of conceptual and legal uncertainty of cyber terrorism as an atypical form of terrorism in general. In turn, such uncertainty generates risks of inadequate response from both the authorities in terms of the optimal (sufficient) legal regulation of relations in the field of countering current and potential cyber threats and the prospective development of general prevention measures. The situation is aggravated by the fact that in the modern conditions of the fight against terrorism, its universal definition has not yet been developed.

The Convention Mechanism for Countering Terrorism is represented by many international treaties of a universal and regional character. Currently, 40 "anti-terrorist" international treaties have been concluded, including 18 treaties signed within the framework of lawmaking work under the auspices of the United Nations, and 22 regional documents. Many issues regarding interstate cooperation and the development of national measures in the fight against terrorism are reflected in special declarations and UN resolutions. In this regard, the problem of adequately defining the legal parameters of cyber terrorism, which acts as a form of political violence derived from traditional terrorism, is actualized. Noteworthy is the fact that international regional conventions on cybercrime (COUNCIL OF EUROPE CONVENTION OF 2001; AFRICAN UNION CONVENTION OF 2014; CONVENTION OF THE LEAGUE OF ARAB STATES OF 2010, reflecting the criminalization of acts committed in the field of computer information, only in some cases consolidate the contextual connection of crimes in the field of information technology with certain manifestations of terrorism.

LITERATURE REVIEW AND RESEARCH METHODS

The paper analyses domestic and foreign views on the political and legal essence of cyberterrorism as an atypical (derivative) form of traditional terrorism. Among domestic scientists in the field of criminology and criminal law, two groups of researchers can be distinguished who either focus on the outer side of cyber terrorism (RUBANOV, 2011; URAZBAEV, 2007), or on its inner side (VASENIN, 2004; CHERNYADYEVA, 2017). Some authors (DREMLYUGA, KOROBEYEV, FEDOROV, 2017) argue the need for a broader approach to cyber terrorism, in which the general concept of "cyber terrorism" should cover, on the one hand, directly cyberattacks (terrorist cyberattacks), and, on the other hand, all other actions performed through the information and communication environment to support terrorism. Comparative analysis of scientific views on the understanding of cyberterrorism proposed by foreign researchers (DENNING, n.d., 2007; HUA & BAPNA, 2012; BOSCH, 2004; SHARP PARKER, 2010) ; SHINDER, 2020; CLOUGH, 2015; KRASAVIN, n.d.), allows us to see the general and special constitutive aspects of the phenomenon in question. Some scientists (DINSTEIN,2015; LILIENTHAL, 2015; BROWNLIE, 1963) conclude that in the modern conditions of the scientific and technological progress development, certain negative manifestations of international relations committed in the information environment can be considered as illegal acts (from the standpoint of international criminal law).

The method of analysis (which made it possible to isolate and study individual aspects of the phenomenon under consideration), the method of transition from abstraction to concretization (in terms of formulating a more accurate definition of cyber terrorism), and the method of deduction, which presupposes leading thought from general provisions to particular conclusions (certain conclusions were drawn on the topic on the basis of the analysis,) were used as the methods of this study.

DISCUSSION REGARDING A COMMON DEFINITION OF CYBER TERRORISM

Despite the wide coverage of the problems concerning the spread of cyber terrorism combined with the low efficiency of national law enforcement systems in countering it, a single concept of this phenomenon has not yet been developed. The complexity of the phenomenon under consideration in terms of definitive identification is evidenced by the wide range of concepts of cyber terrorism presented in the academic sphere and expressing the different essence of this phenomenon. It will be indicative to note that terrorism as an interdisciplinary

(and multicultural, to a certain extent) phenomenon of social reality manifested in the information space through the intensive use of ICT is often defined in different ways depending on the chosen paradigm of thinking and the instrumental-functional approach. In this aspect, this object begins to be considered from the standpoint of general ideas or particular ideas prevailing in the academic sphere, which predetermines terminological confusion in terms of convergence with such concepts as cyber intervention, cyberattack, cyber war, cyber incident, and cyber aggression (KERSCHISCHNIG, 2012).

At the same time, these concepts reflect the real phenomena of social reality manifested in the information and communication space, which, in turn, is an independent sphere of political and legal interaction among the subjects of international relations in modern conditions of the scientific and technological progress development. For example, interference in the internal affairs of another state, a state of war between states, aggression against a sovereign state, sabotage, an unfriendly act today is manifested in the information and communication space using ICT. The media and scientific research increasingly offer different options for political understanding and legal qualifications of negative manifestations of international relations committed in the information environment (DINSTEIN, 2015).

However, overall, there is a relative unity (albeit with separate reservations) in the understanding that such acts can give rise to consequences correlated in the nature and degree of public danger with similar acts that occur in the physical world. In other words, if today, from the position of de lege lata, it is customary to distinguish terrorism from the crime of aggression, and to distinguish the crime of aggression from an unfriendly act and actions that constitute interference in the internal affairs of another state, then it is necessary to delimit and identify these actions (committed in cyberspace) as independent phenomena in the information and communication sphere from the standpoint of the rules of legal qualification and formal logic,.

In addition, cyber terrorism also needs to be distinguished from cybercrime being a broader concept. In the academic sphere, there is also no certainty on this issue, since those autochthonous concepts are quite often used, which reveal the etymological meaning of the phenomenon under consideration, with the assumption of some relevance in relation to the sphere used. Cybercrimes are often defined through terms such as "computer crimes", "computer-related crimes", "computer-assisted crimes." In the context of the development of information and communication technologies, one can find the identification of cybercrimes with high technologies, digital, electronic, virtual, technological and high-tech illegal acts (COMPUTER CRIME, 2001)

It seems appropriate for the purposes of this study to conduct a review analysis of the main definitions with the subsequent construction of the final definition of this phenomenon without pretending to a substantive analysis and detailed coverage of various author's proposals regarding the phenomenon of cyber terrorism. First of all, we would like to note that the concept of "cyber terrorism" was first introduced into scientific circulation in the 1980s by Barry Collins, an employee of the American Institute for Security and Intelligence, who proposed only a general approach to defining this phenomenon, which assumes the convergence of terrorism and cybernetics. Around the same time, FBI Special Agent Mark Pollitt proposed a working definition of cyber terrorism, which was to be understood as a deliberate, politically motivated attack against information, computer systems, computer programs and data that is the result of violent actions against non-military targets by subnational groups or covert agents (KRASAVIN, n.d.). In the future, this definition has undergone repeated changes associated with the expansion of the content side through the specification or addition of individual features of this phenomenon, which predetermined various conceptual approaches in formulating the most acceptable definition.

A generalization of relevant definitions of cyber terrorism takes place within the framework of the first approach, contributing to the disclosure of this phenomenon through unlawful attacks or threats of attacks against information, computer systems, computer programs and data committed for political, ideological, religious or other reasons to compel the authorities to facilitate in achieving political or social goals (KRASAVIN, n.d.; DENNING, n.d., 2007). Cyber terrorism is a collection of illegal actions in cyberspace that contribute to the creation of fear

and tension in a society to gain an advantage in solving political, economic or social problems. Subsequently, the proposed definition of cyber terrorism was expanded to include non-state actors who carry out cyberattacks (or threats of such attacks) against information systems to intimidate or coerce official authorities or society to achieve political or social goals.

Among the advantages of this approach in defining cyberterrorism, it should be noted that, in terms of content, the goals and motives of illegal activity are concretized, which ultimately determine an immanent link with the more general concept of terrorism. It is proposed that this approach should be recognized on this basis as defining in the qualification of a criminal act as a cyber-attack, since this allows it to be distinguished from similar, but less dangerous phenomena (CHERNYADYEVA, 2017).

In fact, one cannot but agree with this position due to the social nature of terrorism, expressed in the orientation of criminal violence towards achieving criminal goals by creating an atmosphere of fear and influencing the authorities based on the motives inherent in the ideology of terrorism. This approach makes it possible to distinguish cyber terrorism from other unlawful acts committed in the information and communication environment, which, when their external signs of the act coincide (actus reus), at the same time differ in their subjective side (mens rea). For example, a DDoS attack on the banking system servers can be organized for different motives and pursue different goals: by competitors, with the aim of damaging business reputation; attackers (hackers) with the aim of stealing money; political opponents, with the aim of undermining the financial system; terrorists, to destabilize the situation in the region by intimidating the population and influencing the authorities (BUTKOV, 2015).

At the same time, it is necessary to understand that the motives of the crime should not be considered in its pure form as an internal motivation that guides a person to commit certain illegal acts, regardless of the registration of goals. Accordingly, goal setting also presupposes the choice of adequate means to achieve the planned result. Based on these considerations, it becomes possible to distinguish by the nature of public danger between politically motivated unlawful acts in cyberspace of varying intensity, which in some cases can be considered as a form of terrorism (cyber terrorism), and in others as hacktivism. The latter is understood as the illegal commission of computer operations with the help of special software (information hacking tools) associated with civil disobedience in cyberspace (DENNING, n.d., 2007). Basically, hacktivism means low-level computer network attacks or digital activity, which in most cases only cause temporary inconvenience. Like cyber terrorists, hacktivists pursue political goals, but their activities, both quantitatively and qualitatively, do not correspond to the possible result of cyberattacks (SHINDER, 2020). The literature rightly notes that hacktivism (hacking, worms, computer viruses, spam, phishing, damage to websites and theft of personal data) is not a manifestation of cyber terrorism, but in the presence of additional conditions, it can act as a functional element of cyber terrorism (SHARP PARKER, 2010).

The second approach is largely based on the first one, with the only difference that the conceptual definiteness of cyber terrorism encompasses the specification of its objective side (attention to the external side of manifestation is updated). Thus, a number of Russian scientists (RUBANOV, 2011) consider cyber terrorism as certain actions (attacks) committed against computer information in critical segments of the state and in the private sector, as well as against a computer system or network. The external side of such actions is expressed in the illegal use of information technologies and the capabilities of the information system, which create the danger of death of people, causing significant property damage or the onset of other socially dangerous consequences.

The relevant definition of cyber terrorism within the framework of this approach can be presented as targeted attacks carried out through the use of computers, information technologies and the capabilities of the information system as a whole, creating the danger of death to people, causing significant property damage or the onset of other socially dangerous consequences, in order to intimidate or kill peaceful residents or to cause large-scale destruction or undermining of political institutions of power (BOSCH, 2017). This form of terrorism involves the use of computers and related equipment to cause massive disruptions in the flow of information or services in order to create an atmosphere of fear or undermine

public confidence in key public institutions and critical national infrastructure (https://www.sipri.org).

From the standpoint of actus reus, cyber terrorism within the framework of this approach can be expressed in such actions as theft or destruction of information, software and technical resources of strategic importance by overcoming protection systems, introducing viruses, software bugs; damage to individual physical elements (for example, the destruction of power supply networks, the temporary disabling of individual sites, jamming them, the use of special programs that stimulate the destruction of hardware, as well as biological and chemical agents to destroy the element base); impact on software and information with the aim of distorting or modifying them in information systems and control systems; destruction or active suppression of communication lines, erroneous addressing, artificial overload of switching nodes; disclosure and threat of publication of classified information about the functioning of the information infrastructure of the state, socially significant and military information systems, encryption codes, principles of encryption systems; remote seizure of telecommunication broadcasting channels for the purpose of spreading disinformation, rumours, demonstrating the power of a terrorist organization and announcing their demands; influence on operators, developers, operators of information and telecommunication systems in order to commit erroneous actions; a false threat of an act of cyber terrorism with serious economic consequences (ZHURAVEL, 2018).

Some experts in the legal field note the impossibility of defining cyber terrorism exclusively in the form of a kind of terrorist act and justify the need for a broader approach, according to which cyber terrorism should cover terrorist acts committed through the use of remote information and communication technologies on the Internet to harm public interests and actions that are committed in support of terrorism through the abuse of the Internet (DREMLIUGA et al., 2017). The latter includes the propaganda of terrorist practices and ideology; inducement, recruitment or other involvement of a person in the commission of terrorist crimes; training of persons for terrorist purposes; financing of terrorism; justification of terrorism, as well as public calls for terrorist activity; communication in social networks.

These acts are also committed in the digital information environment and are associated with the creation of conditions for the implementation of acts of terrorism in the future. These conditions include the creation of a favourable socio-psychological climate that justifies, explains and stimulates illegal activities. The actions aimed at collecting funds on the Internet testify to the creation of material conditions for carrying out terrorist attacks, since they allow accumulating the necessary funds to prepare and carry out planned acts of terrorism in the future. In addition, Internet resources can also be used to provide appropriate communications between terrorist groups and individual terrorists. While examining the correlation between various forms of terrorist activity on the Internet, Jonathan Clough concludes anonymous email accounts and encryption can be used to disguise terrorist communication; websites can be used to spread propaganda or recruit members, and the Internet itself can act as a way to collect the information they need (CLOUGH, 2015, p.12).

The scientific literature also notes the possibility of a differentiated approach in defining cyber terrorism. According to E. Rogovsky, there are two types of cyber terrorism: the direct commission of terrorist actions using computers and computer networks and the use of cyberspace by terrorist groups for organizational and communication purposes and for the purpose of blackmail, but not for the direct commission of terrorist acts (ROGOVSKY, 2007).

In general, it can be noted that the expanded approach in defining cyber terrorism is consistent with international practice of countering terrorism in the information space. In this aspect, attention is drawn to the official report of the UN Office on Drugs and Crime, in which the concept of "cyber terrorism" covers various crimes of a terrorist nature (in particular, propaganda (use of the Internet for recruitment, incitement and radicalization), funding, training, planning, spreading threats, the implementation of the terrorist act itself) that are committed in the information space and (or) with the help of information and communication technologies (THE USE OF THE INTERNET FOR TERRORIST PURPOSES, 2012).

CONCLUSIONS

Based on the analysis of doctrinal ideas regarding the conceptual and legal essence of cyberterrorism, we can conclude that there is no generally accepted definition of cyberterrorism in the domestic and foreign doctrine as a type of information threat manifested in the Internet. Analysis and generalization of scientific positions regarding the development of an optimal definition of cyber terrorism highlight only the general contours of the phenomenon under consideration, according to which cyber terrorism (cyberattack) is defined as an illegal use of information and communication technologies in relation to computer information, computer systems and networks in critical segments of the state and in the private sector that create the danger of death of people, causing significant property damage or the onset of other socially dangerous consequences with the aim of aggravating fear and tension, as well as influencing the authorities for political or other motives, characteristic of the ideology of terrorism. It should be noted that in the legal field, attempts are being made to expand the understanding of cyber terrorism, encompassing both cyberattacks against computer information, computer systems and networks, and other types of illegal activities to support terrorism through the abuse of the Internet (in particular, the propaganda of ideas of terrorism, incitement, recruitment, financing, training, planning, threat propagation).

REFERENCES

AFRICAN UNION CONVENTION OF 2014 [Electronic source]. Available at: https://au.int/sites/default/files/treaties/29560-treaty-0048-african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. Access: 20 May 2020.

AKHGAR, B.; BREWSTER, B. *Combatting cybercrime and cyberterrorism.* Challenges, Trends and Priorities / B. Akhgar, B. Brewster. Springer International Publishing Switzerland. 2016.

ASHRAF, D.A.; FILIPPIDOU, D.A. *Terrorism and Technology.* [Electronic source] Centre of Excellence Defence against Terrorism. Available at: https://www.researchgate.net/publication/330039460_Terrorism_and_Technology. Access: 20 May 2020.

BLANCK, L.R. International law and cyber threats from non-states actors. *International Law Studies,* 89(406), 406-437, 2013.

BOSCH, O. Defending against cyber terrorism: preserving the legitimate economy. In: Bailes, A. J.K and Frommelt, I. (eds.), *Business and security:* public– private sector relationships in a new security environment. SIPRI and Oxford University Press, p. 187–96, 2004. http://books.sipri.org/files/books/SIPRI04BaiFro/SIPRI04BaiFro16.pdf. Access: 20 May 2020.

BROWNLIE, L. *International law and the use of force by states.* UK: Clarendon, 1963.

BYTKOV, P.P. *Terrorism and security problems in the modern world.* P.P. Butkov, A.I. Zaitsev. SPb.: Publishing house of the Polytechnic University, 2015.

CHERNYADYEVA, N.A. *International terror:* origin, evolution, topical issues of legal counteraction. Monograph. Moscow: Prospect, 2017.

CLOUGH, J. *Principles of cybercrime.* Cambridge University Press. 2015.

COMPUTER CRIME. *A join report,* 2001. [Electronic source]. Available at: https://www.nj.gov/sci/pdf/computer.pdf. Access: 20 May 2020.

CONVENTION OF THE LEAGUE OF ARAB STATES OF 2010 [Electronic source]. Available at: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf. Access: 20 May 2020.

COUNCIL OF EUROPE CONVENTION OF 2001 [Electronic source]. Available at: https://rm.coe.int/1680081561. Access: 20 May 2020.

DENNING, D. A *View of cyberterrorism five years later* [Electronic source]. Naval Postgraduate School. In: HIMMA, K. (Ed.) *Internet Security:* Hacking, Counterhacking, and Society. Jones and Bartlett Publishers, 2007. Available at: https://faculty.nps.edu/dedennin/publications/Cyberterror%202006.pdf. Access: 20 May 2020.

DENNING, D.E. *Activism, hacktivism, and cyberterrorism*: the internet as a tool for influencing foreign policy, n.d. [Electronic source] / Information Warfare Site. Available at: http://www.iwar.org.uk/cyberterror/resources/denning.htm. Access: 20 May 2020.

DINSTEIN, Y. *War, aggression and self-defence.* Fifth Edition. Cambridge University Press, 2015.

DREMLIUGA, R.; KOROBEEV, A.I.; FEDOROV, A.V. Cyberterrorism in Chine: criminal law and criminological aspects. *Russian Journal of Criminology, 11*(3), 607-614, 2017.

HUA, J.; BAPNA, S. How Can We Deter Cyberterrorism? *Information Security Journal: A Global Perspective, 2,* 102-114, 2012.

KAPUSTIN, A.YA. On the issue of the international legal concept of threats to international information security. *Journal of foreign legislation and comparative jurisprudence, 6,* 44-51. 2017.

KERSCHISCHNIG, G. *Cyberthreats and International Law.* The Hague, 2012.

KRASAVIN, S. What is cyber-terrorism? [Electronic source]. Computer Crime Research, n.d. Center. Available at: http://www.crime-research.org/library/Cyber-terrorism.htm. Access: 20 May 2020.

LILIENTHAL, G.; NEHALUDDIN, A. Cyber-attack as inevitable kinetic war. *Computer Law & Security Review, 31*(3), 2015.

ROGOVSKIY, E.A. Russia in the fight against international terrorism: the verge of enhancing the country's positive image. *Russia and America in the XXI century, 3,* 2007.

RUBANOV, A.V. *On the coordination of processes of international cooperation and national interests in the field of information security* [Electronic source]. Available at: http://www.agentura.ru/equipment/psih/info/conferencepole/rubanov/.2011. Access: 20 May 2020.

SHARP PARKER, A.M. *Cyberterrorism:* an examination of the preparedness of north carolina local law enforcement. *Security Journal, 23*,159-173, 2010.

SHINDER, D.L. *Scene of the cybercrime:* computer forensics handbook. Syngress. Rockland (MA), USA, 2020.

THE USE OF THE INTERNET FOR TERRORIST PURPOSES (New York: United Nations, 2012), 3–12. [Electronic source]. Available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf. Access: 20 May 2020.

URAZBAEV A. *Cyberterrorism:* problems of counteraction [Electronic source]. Available at: http://viperson.ru/wind.php?ID=565570 .2007.

VASENIN, V. A. *Tsentr issledovaniya komp'yuternoy prestupnosti* [Computer crime research center], 2004 [Electronic source]. Available at: http://www.crime-research.ru/articles/vasenin. Access: 20 May 2020.

ZHURAVEL, V. Countering the threat of cyberterrorism. *Foreign military review, 5*, 12-15. 2018.

Doctrinal comprehension of cyber terrorism in the context of intensive development of information and communication technologies in the modern world

Compreensão doutrinária do terrorismo cibernético no contexto do intenso desenvolvimento das tecnologias de informação e comunicação no mundo moderno

Comprensión doctrinal del ciber terrorismo en el contexto del desarrollo intensivo de las tecnologías de la información y las comunicaciones en el mundo moderno

Resumo

O artigo examina os aspectos doutrinários da compreensão do terrorismo cibernético como uma manifestação (forma) atípica do terrorismo tradicional, atualizado à luz do intenso desenvolvimento e ampla disseminação das tecnologias de informação e comunicação (TIC) no mundo moderno. A conclusão é fundamentada que o terrorismo cibernético é um conceito conceitualmente relevante, que é percebido como um método de cometer um ato terrorista (compreensão reduzida), ou como quaisquer crimes de natureza terrorista que são cometidos usando tecnologias de informação e comunicação (amplo entendimento). A análise e generalização das posições científicas nos permitiu definir este fenômeno da realidade social como o uso ilegal de tecnologias de informação e comunicação em relação à informação, sistemas e redes de computadores em segmentos críticos do Estado e do setor privado, que representam risco de morte, causando danos materiais significativos ou o desencadeamento de outras consequências socialmente perigosas, com o objetivo de suscitar medo e tensão, bem como influenciar as autoridades por motivos políticos ou outros característica da ideologia do terrorismo,

Palavras-chave: Terrorismo cibernético. Crime cibernético. Segurança da informação. Hacktivismo.

Abstract

The paper examines the doctrinal aspects of understanding cyber terrorism as an atypical manifestation (form) of traditional terrorism updated in light of the intensive development and widespread dissemination of information and communication technologies (ICT) in the modern world. The conclusion is substantiated that cyber terrorism is a conceptually relevant concept, which is perceived either as a method of committing a terrorist act (reduced understanding), or as any crimes of a terrorist nature that are committed using information and communication technologies (broad understanding). Analysis and generalization of scientific positions allowed us to define this phenomenon of social reality as the illegal use of information and communication technologies in relation to computer information, computer systems and networks in critical segments of the state and in the private sector, which pose a risk of death, causing significant property damage or the onset of other socially dangerous consequences, with the aim of whipping up fear and tension, as well as influencing the authorities for political or other motives characteristic of the ideology of terrorism.

Keywords: Cyber terrorism. Cybercrime. Information security. Hacktivism.

Resumen

El artículo examina los aspectos doctrinales de la comprensión del terrorismo cibernético como una manifestación (forma) atípica del terrorismo tradicional actualizado a la luz del desarrollo intensivo y la difusión generalizada de las tecnologías de la información y la comunicación (TIC) en el mundo moderno. Se sustenta la conclusión de que el terrorismo cibernético es un concepto conceptualmente relevante, que se percibe como un método para cometer un acto terrorista (comprensión reducida) o como cualquier delito de carácter terrorista que se cometa mediante el uso de tecnologías de la información y la comunicación (208amplio entendimiento). El análisis y generalización de posiciones científicas permitió 208olitic este fenómeno de la realidad social como el uso 208olitic de las tecnologías de la información y la comunicación en relación con la información informática, sistemas informáticos y redes en segmentos críticos. Del Estado y del sector privado, que suponen un riesgo de muerte, provocando importantes daños materiales o la aparición de otras consecuencias socialmente peligrosas, con el objetivo de avivar el miedo y la 208olitic, así como influir en las autoridades por motivos 208oliticos o de otra índole. Característica de la ideología del terrorismo,

Palabras-clave: Ciberterrorismo. Ciberdelincuencia. Seguridad de la información. Hacktivismo.