ppi 201502ZU4645
Publicación científica en formato digital
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185
Depósito legal pp 197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche" de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.40 | Nº 75
2022

Cuestiones Políticas Vol. 40, Nº 75 (2022), 274-284
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Information terrorism as a threat to the global security system of the 21st century

DOI: https://doi.org/10.46398/cuestpol.4075.18

Yuliia Kobets *
Mykola Pogrebytskyi **
Olena Berezovska-Chmil ***
Svitlana Kharchenko ****
Andrey Pravdiuk *****

Abstract

The purpose of the research is information terrorism as a threat to the global security system of the 21st century. The problem of combating information terrorism requires the analysis of the structure of terrorism itself as a phenomenon that has come a long way of evolution from lone suicide bombers, to huge terrorist organizations that commit destructive acts and cause the death of a large number of people, also using the dissemination of information to intimidate a significant number of people. The methodological basis of the research is presented as comparative-legal and systematic analysis, formal-legal method, method of interpretation, hermeneutic method, as well as methods of analysis and synthesis. It is concluded that, one of the main threats to information security is presented by computer terrorism as a form of destructive influence aimed at manipulating or intimidating the population or causing harm to the society, the state or individuals with the use of information technologies and with the purpose of forcing the authorities, an international organization, a natural or legal person (group of persons) to commit a certain action (or refrain from committing it).

* Associate professor, Candidate of Political Science, Department of Political Institutions and Processes, Faculty of History, Politology and International Relations, Vasyl Stefanyk Precarpathian National University. Ukraine. ORCID ID: https://orcid.org/0000-0001-9492-6119

** Professor, doctor of legal sciences, senior researcher, Department of counterintelligence defense of critical infrastructure, professor,National Academy of Security Service of Ukraine , Kyiv Ukraine. ORCID ID: https://orcid.org/0000-0003-0779-6577

*** Associate Professor, Candidate in Political Science, Faculty of History, Political Science and International Relations, Department of Political Institutions and Processes, Vasyl Stefanyk Precarpathian National University. Ukraine. ORCID ID: https://orcid.org/0000-0002-3395-9141

**** Professor of the Department of Journalism and Linguistic Communication, Doctor of Philology, Associate Professor, Faculty of the Humanities and Pedagogy, Department of Journalism and Linguistic Communication, National University of Life and Environmental Sciences of Ukraine. Ukraine. ORCID ID: https://orcid.org/0000-0001-9336-1259

***** Candidate of Law Sciences, Associate Professor, Faculty of Management and Law, Department of Law, Vinnytsia National Agrarian University, Ukraine. ORCID ID https://orcid.org/0000-0002-5248-8111

Recibido el 14/09/22 Aceptado el 16/11/22

Keywords: terrorism; global security system; information technologies; information terrorism; political activity.

El terrorismo informativo como amenaza para el sistema de seguridad global del siglo XXI

Resumen

El propósito de la investigación es el terrorismo de información como una amenaza para el sistema de seguridad global del siglo XXI. El problema de combatir el terrorismo de la información requiere el análisis de la estructura del terrorismo en sí mismo como un fenómeno que ha recorrido un largo camino de evolución desde terroristas suicidas solitarios, hasta enormes organizaciones terroristas que cometen actos destructivos y provocan la muerte de un gran número de personas, usando también la divulgación de información para intimidar a un número significativo de personas. La base metodológica de la investigación se presenta como análisis comparativo-legal y sistemático, método formal-legal, método de interpretación, método hermenéutico, así como métodos de análisis y síntesis. Se concluye que, una de las principales amenazas a la seguridad de la información la presenta el terrorismo informático como una forma de influencia destructiva dirigida a manipular o intimidar a la población o causar daño a la sociedad, al Estado o a los individuos con el uso de las tecnologías de la información y con el propósito de obligar a las autoridades, una organización internacional, una persona física o jurídica (grupo de personas) para cometer una determinada acción (o abstenerse de cometerla).

Palabras clave: terrorismo; sistema de seguridad global; tecnologías de la información; terrorismo de la información; actividad política.

Introduction

The rapid development of information technologies, the scale of applying global telecommunication networks and the process of building an information society have caused new threats in the information sphere; and one of such threats consists in the use of emerging opportunities for terrorist activities that harm vital interests of individuals, the society and the state. In such conditions, the level of information terrorism threat in the information space is growing rapidly.

No doubt that today the Internet has made it difficult to protect information resources. Terrorist groups and individual terrorists all over the world use its features and advantages, trying to influence both the internal and foreign policies of states, using various information technologies to achieve their criminal goals. In the legal literature, it is indicated that availability of information technologies significantly increases risks of information terrorism, and the development of the information infrastructure of the society contributes to creation of additional risks of information terrorism, which in the modern conditions of globalization and internationalization acquires extremely destructive significance.

The problem of combating information terrorism requires analysis of various crisis phenomena and the structure of terrorism itself as a phenomenon that has gone a long way of evolution from lone suicide bombers to huge terrorist organizations committing acts of terrorism and entailing death of a large number of people and to the use of information for intimidating significant numbers of people. Therefore, research of the phenomenon of information terrorism in the context of information security is an important issue of the national security. Information terrorism gives rise to new phenomena that are researched by modern scientists (Filinovych, 2021).

1. Literature review

Despite numerous publications devoted to various aspects of the information terrorism phenomenon, this problem has not yet received proper scientific understanding among scientists and specialists. There is no unity of approaches to understanding this phenomenon. There is still no unified interpretation in the doctrine of information law. Some domestic authors make quite successful attempts to investigate the issue of legal provision of information security (Kuniev, 2021).

If we analyze foreign sources, we can conclude that there are several points of view regarding the problem.

One of them boils down to the fact that "information terrorism" is a sphere of negative influence on individuals, the society and the state with the help of all types of information with the aim of weakening or overthrowing the constitutional order, and that it is a form of negative influence through the use of information and communication technologies (Hlotyna, 2014).

Information terrorism is often viewed exclusively within the intellectual sphere, as one of the most promising types of terrorism that operates in the intellectual sphere and gives rise to a new type of cyberspace-related violence that can be directed against anyone, and its success is ensured not by brute force, but by neurons.

According to another point of view, information terrorism consists in intimidation of the society through the use of high technologies for the purpose of achieving political, religious or ideological goals, as well as in actions leading to disconnection, disabling of critical infrastructure objects or destruction of information (Tafoya, 2011). Such actions may include the use of information technology to organize and execute attacks against telecommunications networks, information systems and communication infrastructure.

A significant contribution to the research of information terrorism as a means of introducing information war was made by foreign scientists. Works by J. Baudrillard, W. Laqueur (1996) A. Toffler (Tafoya, 2011), B. Hofmann, A. Schmidt and others should be pointed out. Analysis of scientific literature shows that most foreign researchers share the point of view that information terrorism is a variety of terrorist activities related to achievements in the sphere of information technologies.

At the same time, there are differences of views among scientists regarding forms and types of information terrorism. There is also a lack of a comprehensive approach to determining the place of information terrorism in the system of threats to the state's national security.

2. Materials and methods

The research is based on the work of foreign and Ukrainian researchers on methodological approaches of understanding principles of law in the contexts of modern globalization transformations.

With the help of the gnoseological method, the essence of methodological approaches to understanding information terrorism as a threat to the global security system was clarified, thanks to the logical-semantic method, the conceptual apparatus was deepened, and the essence of the concepts of information terrorism as a threat to the global security system was determined. Components of methodological approaches of understanding and information terrorism as a threat to the global security system were investigated by means using the system-structural method.

The structural-logical method was used to define the basic directions for optimization of methodological approaches to understanding information terrorism as a threat to the global security system.

3. Results and discussion

Ukrainian researchers and experts also recognize seriousness of danger caused by information terrorism.

So, V.O. Korshunov proposes to understand information terrorism as a new type of terrorist activity focused on the use of various forms and methods of temporary or irreversible disabling the information infrastructure of the state or its separate elements, as well as on the illegal use of the information structure to create conditions that entail grave consequences for various aspects of the life of individuals, the society and the state (Korshunov, 2008).

Law enforcement bodies are obliged to counter threats of information terrorism within their competence. According to K.S. Herasimenko, the main threats in the sphere of information terrorism are mainly created by foreign states, international terrorist organizations and other criminal groups and organizations that take advantage of underdevelopment and weakness of the relevant state structures. Therefore, it is not by chance that there is an opinion that modern information terrorism is characterized as a set of information wars and special operations related to national or transnational criminal structures and special services of foreign states (Herasymenko, 2009).

The Ukrainian legislation does not contain a definition of information terrorism. The Law of Ukraine "On Combating Terrorism" contains the concept of "technological terrorism", which does not coincide with the definition of "information terrorism", and the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" contains a definition of "cyber terrorism", which can be recognized as only one of the varieties of information terrorism, which is discussed below.

Note that the definition of information terrorism is not included in international legal acts such as the Council of Europe Convention on the Prevention of Terrorism (2005), the Convention on Cybercrime (2001).

Generalization of information received from various scientific sources gives grounds to conclude that information terrorism is a doctrinal concept of information security theory which should be understood as follows:

1. a socially dangerous act that is a manifestation of terrorism;
2. a form of destructive informational and psychological influence on individuals, society and the state;
3. dangerous acts of informational influence on social groups of persons, state authorities and management authorities, related to the dissemination of information containing threats of persecution, massacre, murder, as well as distortion of objective information which causes emergence of crisis situations in the state, instilling fear and tension in the society;
4. a certain violent propagandistic influence on a person's psyche, which does not give him/her an opportunity to critically evaluate the information received;

5. a new type of terrorist activity focused on the use of various forms and methods of temporary or irreversible disabling the information infrastructure of the state or its separate elements, as well as on illegal use of the information structure to create conditions that entail serious consequences for various aspects of life of individuals, society and the state (Korshunov, 2008);
6. a number of information wars and information special operations related to national or transnational criminal structures and special services of foreign countries (Herasymenko, 2009);
7. fusion of physical violence with criminal use of information systems, as well as intentional abuse of digital information systems, networks or their components with the aim of facilitating implementation of terrorist operations or actions (Post, 2000);
8. an ideologically based practice of influence aimed at intimidation of the population for decision-making or action (inaction) performed by a government body, a local self-government body, an international organization, a social group, a legal entity or a natural person within the information space related to the use of information, information technologies and/or information resources.

Traditionally, depending on the orientation, two types of information terrorism can be conventionally distinguished: 1) "psychological" one (propaganda of terrorism, creating an atmosphere of fear and panic in society, etc.); 2) "technical" one (control or blocking of mass information transmission channels, disruption of information infrastructure facilities, etc.).

Depending on the criminal goal and the use of tools (means) to achieve it, information terrorism can also be divided into two types: media terrorism and cyberterrorism.

Media terrorism presupposes abuse of information systems, networks, and their components for carrying out terrorist activities (propaganda and dissemination of the terrorism ideology, promotion of terrorist acts). The means of media terrorism include print mass media, broadcast and cable mass media networks, the Internet, e-mail, spam, etc. (Bank, 2016).

Cyber terrorism is a deliberate, politically motivated attack on the objects of the information space; it causes a danger to life and/or health of people or occurrence of other serious consequences, if such actions were carried out with the aim of violating state or public security, intimidating population, provoking a military conflict or a threat of committing such actions. Politically motivated attacks that cause serious damage, such as severe economic hardship or long-term power and water outages, can also be characterized as cyberterrorism.

The Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" defines cyberterrorism as terrorist activity carried out in cyberspace or with its use (Art. 1). Cyberterrorism is a serious socio-political threat to humanity, compared even to nuclear, bacteriological and chemical weapons, and the extent of this threat due to its novelty is not yet fully understood (Bank, 2016). Certain cyber security experts predict that "new terrorists" will direct their efforts to master information weapons with destructive power many times greater than that of biological and chemical weapons (Laqueur, 1996).

World experience shows the indisputable vulnerability of any state, especially since cyber terrorism has no state borders; a cyberterrorist is able to equally threaten information systems located almost anywhere on the globe by using special software designed for unauthorized penetration into computer networks and organizing a remote cyber-attack on the victim's information resources.

The main form of cyberterrorism is information attack by criminal groups or individuals on computer information, computer systems, data transmission equipment, other components of information infrastructure. The consequence of such an attack is penetration into the information and telecommunications network or communication infrastructure, interception of control, suppression of means of network information exchange and implementation of other destructive actions.

Forms and manifestations of information terrorism should be taken into account when determining the status of threats caused by information terrorism but unfortunately not listed in the current legislation of Ukraine (Leheza *et al.*, 2022).

In order to determine such threats, first of all, the essence of the "threat" concept should be clarified. The concept of "threat" should be understood as phenomena and factors that negatively affect or may affect a certain object or pose a danger of violating interests of certain subjects (Tykhonova, 2015).

In accordance with clause 6 Art. 1 of the Law of Ukraine "On the National Security of Ukraine", threats to the national security of Ukraine should be understood as phenomena, trends and factors that make it impossible or difficult or may make impossible or difficult to implement national interests and preserve national values of Ukraine. Literature sources represent various approaches to identification of threats to national security depending on the object of influence.

In particular, one of threats to the national security of a state is called "cyber-threat" as an objective existing possibility of committing cybercrimes resulting in negative consequences for the vital interests of the state in both real and virtual environments (Shelomentsev, 2010). In our opinion, threats in the information sphere should be considered as factors that harm information security of the state. In the draft Concept of the Information Security of Ukraine, threats of an informational nature are defined as existing or potentially possible phenomena and factors that pose a danger to vital interests of individuals and citizens, the society and the state in the information sphere.

Major threats to national security in the information sphere include the following: creation, distribution of information for the purpose of supporting, accompanying or intensifying terrorist activities (subpar. "d" par. 3 Art. 8); manifestations of cybercrime, cyberterrorism (subpar. "b" par. 4 Art. 8).

According to the National Security Strategy of Ukraine the main task of cyber security system development is to guarantee cyber stability and cyber security of the national information infrastructure, in particular in the conditions of digital transformation (par. 52), and priority tasks of law enforcement, special, intelligence and other state bodies include active and effective countermeasures against intelligence and subversive activities, prevention of terrorism, special information operations and cyber-attacks. The Strategy mentions spread of international terrorism in cyberspace as a threat to the national security of Ukraine (Leheza *et al*., 2022).

The information security doctrine does not mention the threat of information terrorism. Among the current threats to information security only special information operations, information expansion, and information dominance are mentioned, although their content of only partially reproduces the concept of information terrorism (Leheza *et al*., 2020).

Obviously, threats of information terrorism should be reflected in the Information Security Strategy of Ukraine, which is provided for by the National Security Strategy of Ukraine (par. 66). This Strategy will determine principles of ensuring information security of Ukraine, countering threats to national security in the information sphere, protecting rights of individuals to information and protecting personal data.

Its purpose is to ensure information security of Ukraine aimed at protecting vital interests of citizens, the society and the state in countering internal and external threats, ensuring protection of the state sovereignty and territorial integrity of Ukraine. Opposition to disinformation, manipulative information, information operations and attacks, including those aimed at committing terrorist acts are defined as a strategic goal № 1 of this Strategy (Leheza *et al*., 2022).

In order to successfully address these threats, a number of key areas should be identified:

- unification and harmonization of national legislation and international acts;

- carrying out scientific developments in the sphere of creating modern technologies for detection and prevention of criminal and terrorist influences on information resources;
- creation of specialized subdivisions in the sphere of fighting computer crimes and computer terrorism;
- improvement of international organizational and legal cooperation on countering computer crime and computer terrorism;
- improvement of multilevel system of personnel training in the sphere of information security (Havrysh, 2009).

Conclusions

In our opinion, one of the main threats to information security in the Information Security Strategy of Ukraine is presented by information terrorism as a form of destructive influence aimed at manipulation or intimidation of population or causing harm to the society, the state or individuals with the use of information technologies for the purpose of forcing the state authorities, an international organization, a legal or physical person (group of persons) to commit a certain action (or refrain from committing it).

Tasks, main principles and directions for improving the state-wide system of combating terrorism in view of modern terrorist threats to the national security of Ukraine and the forecast of their development are determined by the Concept of Combating Terrorism in Ukraine; directions of implementation of this Concept include: identification and analysis of causes and conditions that lead to spread of terrorism; improvement of the legal and organizational framework for combating terrorism; improvement of existing methods as well as development and implementation of new methods for combating terrorism; optimization of ways and methods for protection of life and security, rights and freedoms of people and citizens, protection of interests of the society and the state against terrorist attacks; improvement of informational, scientific, personnel and material-technical support of subjects fighting against terrorism. Information space and its components are identified as objects of possible terrorist attacks.

Bibliographic References

BANK, Rostyslav. 2016. "Information terrorism as a threat to the national security of Ukraine: theoretical and legal aspect" In: Information and law. No. 1, No. 16, pp. 110-116.

FILINOVYCH, Valeriia Viktorivna. 2021. "Cyberstalking: problems of legal protection" In: Scientific works of the National Aviation University. Series: Legal Bulletin «Air and Space Law». Vol. 58. No. 1, pp 135-141.

HAVRYSH, Stepan Bohdanovych. 2009. "Computer terrorism: current state, development forecasts and countermeasures" In: Fight against organized crime and corruption (theory and practice). No. 20, pp. 3-14.

HERASYMENKO, Konstantyn. 2009. Modern signs of threats of «informational terrorism». Law forum. Kharkiv, Ukraine.

HLOTYNA, Yryna Mykhailovna. 2014. Information terrorism and its impact on the economy. economic globalization and problems of national international security. Kyiv, Ukraine.

KORSHUNOV, Vitalii Olehovych. 2008. Political terrorism: informational methods of struggle: abstract of the thesis of a candidate of political sciences. Dnipro, Ukraine.

KUNIEV, Yurii Demianovych. 2021. "Legal provision of information security as a subject of legal research" In: Scientific works of the National Aviation University. Series: Legal Bulletin «Air and Space Law». Vol. 58, No. 1, pp. 95-102.

LAQUEUR, Walter. 1996. "Postmodern Terrorism" In: Foreign Affairs. Vol. 75, No. 5, pp. 24-36.

LEHEZA, Yevhen. 2022. "Illegal influence on the results of sports competitions: comparison with foreign legislation" In: Ratio Juris UNAULA. Vol. 17, No. 34, pp. 53-70.

LEHEZA, Yevhen; FILIPENKO, Tatiana; SOKOLENKO, Olha; DARAHAN, Valerii; KUCHERENKO, Oleksii. 2020. "Ensuring human rights in ukraine: problematic issues and ways of their solution in the social and legal sphere" In: Cuestiones políticas. Vol. 37, No. 64, pp. 123-136.

LEHEZA, Yevhen; SHAMARA, Oleksandr; CHALAVAN, Viktor. 2022. "Principios del poder judicial administrativo en Ucrania" In: *DIXI*. Vol. 24, No. 1, pp. 1-11.

LEHEZA, Yevhen; YERKO, Iryna; KOLOMIICHUK, Viacheslav; LISNIAK, Mariia. 2022. "International Legal and Administrative-Criminal Regulation Of Service Relations" In: Jurnal cita hukum indonesian law journal. Vol. 10 No. 1, pp. 49-60.

POST, Jerrold. 2000. "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism" In: NATO Library at: Terrorismand political violence. Vol. 12, No. 2, pp. 97-122.

SHELOMENTSEV, Volodymyr Petrovych. 2010. "Criminological security in cyberspace: a system of concepts" In: Fight against organized crime and corruption (theory and practice). No. 23, pp. 342-348.

TAFOYA, William. 2011. Cyber Terror. FBI Law Enforcement Bulletin. Available online. In: https://leb.fbi.gov/articles/featured-articles/cyber-terror. Consultation date: 20/05/2022.

TYKHONOVA, Olena. 2015. Financial security of Ukraine: criminal law and criminological foundations. Srednyak T.K. Dnipro, Ukraine.

UNIVERSIDAD DEL ZULIA

CUESTIONES POLÍTICAS

Vol.40 Nº 75

*Esta revista fue editada en formato digital y publicada en diciembre de 2022, por el **Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org