DOI: https://doi.org/10.34069/AI/2021.40.04.8

Cyberterrorism as a threat to the cyber security of Ukraine: A discussion of theoretical aspects

Кібертероризм як загроза кібербезпеці України: обговорення теоретичних аспектів

Received: March 2, 2021 Accepted: April 30, 2021

Written by:
Ihor Diorditsa[24]
https://orcid.org/0000-0001-7765-6591
Kateryna Katerynchuk[25]
https://orcid.org/0000-0002-6700-2831
Armenui Telestakova[26]
https://orcid.org/0000-0003-3371-9137
Nataliia Kulak[27]
https://orcid.org/0000-0001-8619-8975
Andrii Nastiuk[28]
https://orcid.org/0000-0002-2014-1084

Abstract

In this article, the authors analyze cyberterrorism as a threat to Ukraine's cyber security. The urgency of the issue declared in the paper is conditioned by the fact that fair number of terrorist acts intende to make harm to the interests of the state, can be committed today both in real world and in cyberspace. As such acts are committed using computer systems and are done in cyberspace, authors propose to define this type of socially dangerous acts as «cyberterrorism». The methodological basis of this study is a set of philosophical, general scientific, special scientific and other methods that are directly applied in legal researches. The authors have done the interpretation of terms making up the conceptual and categorical apparatus of the subject of research. The difference between information terrorism and cyberterrorism has been substantiated by the writers. The emphasis was placed on the necessity to create a Cyber Command that could react fast to challenges in the information security sphere of the state, including acts of cyberterrorism.

Keywords: cyber security, cyberspace, cyberterrorism, information terrorism, Cyber Command.

Анотація

У статті авторами проаналізовано кібертероризм як загрозу кібернетичній безпеці України. Актуальність заявленої у статті проблеми обумовлена тим, що значна низка терористичних діянь, спрямованих на заподіяння шкоди державним інтересам, сьогодні може вчинюватися як в реальному так і в суто кіберпросторі. Оскільки вчинюються подібні дії з використанням комп'ютерних систем і вчинюються у кіберпросторі, вказаний вид суспільно небезпечних діянь нами пропонується визначати як «кібертероризм». Методологічною основою даного дослідження є сукупність філософських, загальнонаукових, спеціальних наукових ті інших методів, які мають своє безпосереднє застосування у юридичних дослідженнях. Здійснено тлумачення термінів, які становлять понятійно-категорійний апарат предмета дослідження. Обґрунтовано різницю між інформаційним тероризмом та кібертероризмом. Акцентовано увагу на необхідності створення кіберкомандування, яке могло б швидко реагувати на виклики в інформаційній сфері безпеки держави у тому числі й на прояви кібертероризму.

Ключові слова: кібербезпека, кіберпростір, кібертероризм, інформаційний тероризм, Кіберкомандування.

[24] Prof., DSc, Kyiv National University of Technologies and Design, Ukraine.
[25] Prof., DSc, Kyiv National University of Technologies and Design, Ukraine.
[26] Associate Prof., PhD, Kyiv National University of Technologies and Design, Ukraine.
[27] Associate Prof., PhD, Kyiv National University of Technologies and Design, Ukraine.
[28] Associate Prof., PhD, Academy of Labor, Social Relations and Tourism, Ukraine.

Introduction

The importance of information has increased in the modern society. Information has gained value not only in terms of state secrets, but also in terms of commercial secrets, confidential information, personal data. Due to digital civilization development, significant expansion of various software tools utilization in everyday life, large-scale penetration of automation to professional activities has taken place along with, network communications, visualization and data processing penetration into the economy. At the same time, information and knowledge are viewed as intellectual capital, as a commodity that has its value. As the information society is formed, economic security level of the state will be increasingly determined by the ability to implement information and communication technologies in the economic, social, military, technological and cultural spheres of the society. Therefore, the issues of ensuring the interrelationship between economic and information security, including cyber security of the state, commands great attention of the professionals dealing with information technology, economics, politics, law and international relations.

As emphasized in the Okinawa Charter of Global Information Society, information and communication technologies are one of the most important factors influencing 21st century's society formation. Their revolutionary effect relates to the way people live, their education and work, as well as impacts on the interaction between government and civil society. Information technologies quite fast become a crucial stimulus to the world economy development (Ministry of Foreign Affairs of Japan, 2000).

At the same time, computerization processes are rapidly developing in society, and together with all their advantages, have created fair amount of new issues, challenges and threats in the national security domain. This mostly concerns information threats of a terrorist nature. Until the 1990s, terrorism was talked about as a local phenomenon only, however now it has become a global phenomenon, and the role of information technology, especially in acts of terrorism ostentation realization, is becoming increasingly important. Among others, cyberterrorism is becoming a separate type of terrorism, which actually correlates with virtual world development and information flows simulacrum creation. In our days researchers can see that attention to cyberterrorism combating issues is growing rapidly, while many issues remain uninvestigated from the standpoint of legal sciences, which justifies *the relevance of cyberterrorism consideration as a threat to cybersecurity of Ukraine*.

Literature Review

Working on the article the authors have used the scientific achievements of both foreign researchers and the works of the national scientists dealing with terrorism and cyberterrorism. The authors would like to give prominence to the scientific school of Doctor of Law *V. A. Lipkan* (Lipkan, 2008; Lipkan, Maksimenko & Zhelikhovsky, 2006; Lipkan, & Baskakov, 2011), the researchers of said school have dealt with the issues of fighting against terrorism, national security of Ukraine, the legal framework for the information society development in Ukraine (as it is information society where cyberterrorism acts) and information security of Ukraine.

State information security issues have been also investigated in the scientific papers of the following scientists: *O. V. Kubyshkin* (Kubyshkin, 2002), *V. L. Burayachok*, *V. B. Tolubko*, *V. O. Khoroshko & S. V. Tolyupa* (Burayachok, Tolubko, Khoroshko & Tolyupa, 2015). The authors have also used the publications of the following contributors to cyber security and cyberterrorism issues research: *O. G. Shyrokova-Murarash*, *Yu. P. Akchurin* (Shyrokova-Murarash, & Akchurin, 2011), *V. V. Topchiy* (Topchiy, 2015), *G. V. Foros, A. V. Foros* (Foros, & Foros, 2010), *Ie. A. Makarenko* (Makarenko, 2011) and *V. K. Hryzchuk* (Hryzchuk, 2011). Special consideration has been given to the works of *R. Cohen-Almagor* (Cohen-Almagor, 2005), *L. M. Lux* (Lux, 2018), *M. D. Cavelty* (Cavelty, 2018), *S. Berner* (Berner, 2003), *L. Jarvis & S. Macdonald* (Lee & Macdonald, 2015), *G. Weimann* (Weimann, 2004), *S. M. Furnell & M. J. Warren* (Furnell, and Warren, 1999), *W. Tafoya* (Tafoya, 2011) *J. Lewis* (Lewis, 2002) et al.

Methodology

Counter-terrorism efforts in Internet cannot be done without a comprehensive interdisciplinary approach that combines political, legal, technological, media and sociological methods (Zelenkov et al., 2020). In order to carry out innovative research in cybersecurity field, it is necessary to combine knowledge at the intersection between technical and social. Knowledge (and uncertainty) about cybersecurity vulnerabilities lies at this intersection (Cavelty, 2018).

The methodological basis of this research is a set of philosophical, general scientific, special scientific methods that have their direct application in the legal research. Among the general scientific methods used, the major one is the dialectical method of scientific cognition, application of which has allowed studying the continuous development, qualitative changes and relationships between the combat with cyberterrorism and state cybersecurity provision. The methods of legal linguistics, legal hermeneutics and logical-semantic analysis are used to clarify the content or to formulate the basic concepts of this research: «terrorism», «terror», «cyberterrorism», «information terrorism», «terrorist activity», «act of terrorism». System analysis method application allowed us to establish the role of the legal and regulatory definition of cyberterrorism as the legal basis of the state cybersecurity policy in combating cybercrime. The grouping method and the system-structural approach were used for classification division, internal structure clarification along with the analysis of the interrelationships of cyberterrorism elements, and simulation, analysis and synthesis methods – to work out the proposals towards counter-cyberterrorism.

Results and Discussion

Features of the conceptual and categical framework of cyberterrorism in Ukraine and Globally

First of all, it is necessary to be clear about conceptual and categorical framework. Let us emphasize that scientists and practitioners have not reached the agreement towards terminological definition of terrorist activity carried out in cyberspace or using this space – cyberterrorism.

Significant differences can be seen over cyberterrorism within the European Union's research community. In particular, there is no significant consensus regarding the extent to which this phenomenon threatens the security as well as towards potential targets of cyberterrorist attacks (Lee, Macdonald & Nouri, 2014). Researchers L. Jarvis & S. Macdonald have brought about the issue of whether a clear definition of cyberterrorism concept is needed at all, and there was not any unanimous answer and consensus among the respondents (Lee & Macdonald, 2015).

Formal, dogmatic, and hermeneutical analyzes which autors have done gave the possibility to identify different interpretations of cyberterrorism: «information terrorism», «computer terrorism», «cyberterrorism», «technological terrorism», «virtual terrorism», etc. The meaning of these concepts is also defined differently. The difficulty in formulating these concepts obviously exists both due to impossibility to identify a single object of the offence and a sufficiently fair number of the objects of offence in terms of their legal protection.

Here authors are stating our own understanding of the cyberterrorism is a specific term, and information terrorism is a general term of the same social phenomenon. The reason for the fact that information terrorism and cyberterrorism are not the same is their etymological interpretation. Information one refers to information, the one that contains information. Cybernetic is the one that is created and working on the basis of principles, methods of cybernetics. Cybernetics - the science of the general laws of information receipt, storage, transmission and processing (Ieroshenko, 2012).

One group of researchers tends to define cyberterrorism as terrorist activity in which the computer is either the object or an instrument of offence. Researchers of the other group consider terrorist activity using the latest achievements of science and technology in the information technology field to be information terrorism (Foros, Foros, 2010).

Today, offenders can get inside personal computers and computer systems of institutions, enterprises, organizations, including banks, secret services, research institutions, patent agencies, party headquarters, into public computer networks. In addition, the information revolution has made an effect on military affairs. It provided an opportunity to conduct a military campaign in a virtual version. In fact, the war itself can become virtual, although its results will be absolutely real. Information warfare is an example.

The autors would also like to distinct the issue when cyberterrorism is refered also in the event when computer technology was only a means of committing illegal activities and played a supporting role. Under such conditions, researchers can talk about car terrorism, bomb terrorism, bullet or knife terrorism.

In the time of information technology terrorism can be seen as ordinary terrorism, when conventional weapons are used to destroy resources and individuals in the physical sense; techno-terrorism, in which conventional ammunition is used to destroy infrastructure and cause damage in cyberspace; and as cyberterrorism, where new weapons (malware, electromagnetic and microwave weapons) are used to destroy and modify data in cyberspace. The element of suddenness is vital for cyberattack, and its dynamics is changing with each passing day. For this reason, the key issue is whether and how is it possible to completely control cyberspace, how to adopt an appropriate legal framework due to the dynamics of cyber procedures and how to find out the offenders, how to stalk and prosecute them (Vilić, 2017).

S. Zulhuda defines cyberterrorism as a new form of the acts of terrorism which causes more harm however less regulated at the legislative level. Cyberterrorism is a global risk requiring global response. We need a common policy and legal framework establishing minimum standards for counter-cyberterrorism. However, the only international convention on the issues related to cyberterrorism is the Convention on Cybercrime, which does not address the outlined issues (Zulhuda, 2020).

Cyberterrorism exists within cyberspace, is committed in cyberspace, and is focused on the objects in cyberspace. This is an important observation for clarifying the difference between cyberterrorism and ordinary terrorism or terrorist activities committed by various means, including computer technologies.

First of all, let us study such category as «*terrorism*». Definition of «*terrorism*» is quite a complicated task. Forms and methods of terrorist activity have been changing significantly with time passing. This phenomenon has a persistent negative assessment, which evokes arbitrary interpretation. On the one hand, there is a tendency for a broad interpretation, when some political forces for no good reason call their opponents terrorists. On the other hand – narrowing. The terrorists themselves tend to call themselves soldiers, bush fighters, demolitionists in the enemy's rear, etc. This entails difficulties of both legal definitions and general theoretical understanding of terrorism. So far, legislators of the various countries have not reached a common understanding concerning the definition of terrorism.

Historically, the term «terrorism» first appeared in 1798, when the philosopher Emmanuel Kant used it to describe a pessimistic view of human destiny. In the same year, the term appeared in an appendix to the Dictionary of the French Academy, caused by the excesses of revolutionary terror, thus the term did not have the meaning we attribute it today. Presently this term in most cases refers to the actions of various movements that affect the government in order to radically change its political and social governance, when the object of influence is not only the state itself, but also the internal social system (Kubyshkin, 2002), as well as information security in general.

Using the national legal framework, let us note that *terrorism* is understood in it as socially dangerous activity that involves the deliberate, targeted use of violence by taking hostages, arsons, murders, tortures, intimidation of the population and the authorities, or other encroachments on the lives or health of innocent people, or threats to commit criminal acts in order to achieve criminal goals (Law No. 638-IV, 2003).

Terrorist activities are the activities that include: planning, organization, preparation and implementation of terrorist acts; incitement to commit acts of terror, violence over individuals or organizations, destruction of material objects for terrorist purposes; organization of illegal armed groups, criminal groups (criminal organizations), organized criminal groups to commit terrorist acts, as well as participation in such acts; recruitment, arming, training and use of terrorists; terrorist ideology propaganda and dissemination; financing of knowingly terrorist groups (organizations) or other kinds of their support (Law No. 638-IV, 2003). Regarding the international interpretation of this category, even the International Convention for the Suppression of the Financing of Terrorism and the International Convention for the Suppression of Acts of Nuclear Terrorism do not contain a unified definition.

In the Explanatory Dictionary of the Ukrainian language «*terrorism*» is defined as the commission, use of terror; activity and tactics of terrorists. *Terror* is the acutest form of fight against political and class opponents applying violence up to physical destruction (Ieroshenko, 2012).

The existence of terrorism makes provisions for mandatory combination of the principle of harm, teleological (terrorism must be committed in order to change the constitutional order or overthrow a legitimately elected government) and instrumental elements (implanting fear to the people's mind). In the absence of one or several of these requirements, we cannot take up the position that terrorism exists. It is the availability of all these three requirements that distinguishes terrorism from the other acts, whether they are criminal or not, such as threats or a «crime of hatred» (Boeckmann, & Turpin-Petrosino, 2002). The consequences of such horrification can cause cyberparanoia or cyberfear (Mason, Stevenson, & Freedman, 2014).

Quite often terrorism is construed as a background for other international crimes. However, terrorism as a social phenomenon, although it is a crime, requires separate consideration, as it has significant specific feature compared to other crimes, primarily because of its political focus. However, research done by Eriksson, J., & Giacomello, G. establsihed that cybersecurity studies in political science is a marginalized topic, and only one of the top three journals in political science/international relations has published the papers on cybersecurity issues (Eriksson, & Giacomello, 2006).

This specificity results in a special regime to fight against terrorism. As for information terrorism or cyberterrorism, the specificity of the field of action - the information realm - further distinguishes information terrorism from cybercrime. The authors support the scientific view that information terrorism should be considered apart from computer crimes.

First voice of concern about the possible consequences of using the global web was given in 1993 by Alvin Toffler, when the general public had little knowledge about the internet (Shyrokova-Murarash, & Akchurin, 2011). Even at that time Toffler has already predicted that terrorists would try to strike at the information and telecommunications infrastructure of the United States. Since then, a fair amount of studies has been conducted, and experts' opinions on the concept of «cyberterrorism» are diametrically opposed.

However, in case the state does not take steps to facilitate developing of the appropriate technical means of protection against cyber threats, we will quickly realize that the threats of the internet can be compared to environmental pollution and that cyber security in facts demonstrates strong features of the public good that will not be provided or will not be provided at all at the private market (Cavelty, 2007).

Definitions of information terrorism or cyberterrorism can be found both in international legal instruments and draft conventions, as well as in research done by professionals in this issue. One of the characteristic features of the definitions of information terrorism is that the vast majority of them mention only one aspect of information security, namely: related to the data processing means, that narrows the concept of information terrorism, hence limits the scope of legal regulation preventing effective cooperation of states in their combat against information terrorism. However, let us emphasize the fact that for the time being generally accepted definition does not exist and in theoretical respect it is about integration of such concepts as «terrorism» and «computer crime» (Sokur, 2010).

So, authors suggest review in details the existing doctrinal definitions.

Scientific and technological progress, creating new information technologies, within a short time has revolutionary transformed the processes of data creation, collection, receipt, storage, use, dissemination, security and protection. Today criminals quite often use the results of this progress. Penetration to the information sphere and its use by criminal, including terrorist, elements has given rise to phenomena called cybercrime and cyberterrorism. That is, the internet is a breeding ground for (cyber) terrorist attacks coordination (Berner, 2003).

Rafael Cohen-Almagor from the University of Haifa notes that violent movements and individuals use democratic tools to find «golden paths» (from their point of view) to reach their goals without following the rule of law. The subjects of terrorism would be immediately broken up if they used similar tactics in autocratic systems (Cohen-Almagor, 2005).

By its component parts, cyberterrorism should be realized with the specific purpose of changing the constitutional order or overthrowing a legitimately elected government; and should be carried out in such a way as to implant terror to the minds of the people, affirming the belief that anyone anywhere can become the victim of an attack. Eventually, cyberterrorism poses several challenges in a global and technologically interconnected world. Cyberterrorism provides for internet use, which offers a number of benefits to those involved in crime. In addition, since the real size and potential of cyberterrorism are not clear yet, it is quite difficult to respond to such a crime preparation (Lux, 2018).

Cyberterrorism is the «attacks» on computer systems. The means and methods of cyberattacks have been mastered long ago by international extremist organizations as well as national separatist movements. The first examples of «computer terrorism» appeared in the late 1990s, due to the development of computer networks and the growing role of computers in all spheres of life. As a result, they attracted the attention of the various «cyber-hooligans» and «cyber-terrorists» attacking them through unauthorized access to interfere with the normal operation of relevant institutions.

G. Weimann identifies five factors that make cyberattacks attractive to terrorists. These include relatively low financial cost indicators; the prospect of anonymity; wider choice of available targets; ability to carry out attacks remotely; and the potential for scores of victims (Weimann, 2004).

Comparing the harmful consequences due to hackers and cyber-terrorists activities, S. Furnell and M. Warren have noted back in 1999 that cyber-terrorists were politically motivated and that these types of attacks would be more specifically focused and targeted at critical infrastructure and would do more harm than hackers' activities. There are also funding issues, as terrorist groups can have available a good deal of money meaning that they can easily hire hackers to act on their behalf (Furnell, and Warren, 1999).

By *cyberterrorism* is meant deliberate motivated attack on information processed by a computer, on computer system or network; it is associated with danger to human life and health or the occurrence of other serious consequences, provided that such actions are committed to violate public safety, intimidate the population, provoke military conflict. The *Law of Ukraine «On Basic Principles of Cyber Security of Ukraine»* defines «cyberterrorism as terrorist activity conducted in cyberspace or using it» (Law No. 2163-VIII, 2017). Concerning the international formalization of this term, Convention on Cybercrime of the Council of Europe does not contain particular definition of cyberterrorism.

The provisions of the *«Convention on Cybercrime» of the Council of Europe* are represented in the Law «On Amendments to the Criminal and Criminal and Procedure Codes of Ukraine» dated 23.12.2004, according to which in section 16 «Crimes in the field of electronic computing machines (computers), systems and computer networks and telecommunication networks application» the Articles 361, 362, 363 of the Criminal Code are amended and restated and criminal liability is provided under the Articles 361-1, 361-2 and 363-1 (Law No. 2289-IV, 2004).

In accordance with the Draft Convention on Strengthening Protection against Cybercrime and Cyberterrorism, *information terrorism or cyberterrorism* is the intentional use of unlawfully established authority, violence, destruction or intrusion into cybersystems, provided that such actions could cause death or harm to a person or persons, essential damage to property, civil disorder or substantial commercial detriment.

In the mid 1980s, Berry Collin, a member of the American Institute for Security and Intelligence, has introduced the term «*cyberterrorism*» to name terrorist acts in cyberspace.

The Center for Strategic and International Studies defines *cyberterrorism* as the use of computer network tools to stop functioning critical national infrastructural facilities (in particular power generating, transport, governmental), or to coerce or intimidate government or civil population (James A. Lewis, 2002).

Cyberterrorism is also defined as intimidation of society through the use of high technology to achieve political, religious or ideological goals, as well as actions causing disconnection of infrastructure facilities or removal of data or information critical for infrastructure facilities (Tafoya, 2011).

For the time being the number of cyberattacks and examples of cyberterrorism is growing fast, and the level of harm is increasing significantly. The major issue here is the lack of clear legislation that would clearly define this concept, provide for liability for illegal acts, which indicates a lack of comprehension of this phenomenon. The difficulty in defining «cyberterrorism» term is mainly caused by the fact that it is challenging to separate cyberterrorism itself from the acts of information war, and it is complicated to separate the use of information weapons from crimes in computer data field or patriotic aspirations of the countries and regions. Incidental difficulties arise while attempting to identify the specific features of this form of terrorism. For example, the psychological and economic aspects of cyberterrorism are closely intertwoven, and it is impossible to unambiguously determine which one overweights.

Cyberterrorism is one of the forms of manipulative influence on the social consciousness, when terrorists use computers, dedicated software, telecommunication networks, as well as modern information technologies to achieve their political and ideological goals and narratives, thus providing unauthorized access to certain information and software resources, technological processes. Demonstration by terrorists their capability to get access to certain resources, facilities and systems and the threat of using this opportunity to cause harm to society affects the psychological state and behaviour of people (Poteriakhina, 2012).

Counterterrorism efforts and state building do not necessarily go hand in hand (Pašagić, 2020). Clearer legal definability, less confrontation, and enhanced cooperation between the governments and private firms will facilitate cleaning up terrorist content (terror nature propaganda) from major web sites, will help stop a number of cyberterrorists, and exonerate technical firms from charges for copartnership with terrorists (Budhijanto, 2019).

The authors of this research are sure that a clear example of such cooperation is capabilities of Clubhouse application for iOS, which was launched in April 2020. Attentive users of this application probably have noticed that the privacy policy of the service states that Clubhouse can record and store conversations for certain time. The reasons for such actions are primarily terrorism and hate language (Cyber Policy Center, 2021).

Cyberterrorism is characterized, first, by the use of a computer or other gadget having access to the network as a tool of crime; second, the existence of the internet as an international information space where the object of the crime is located; third, a malicious attack by criminal individuals or groups of them on specific objects such as data, software, computers, local and global networks.

Terrorism in computer technology sphere has the following characteristic features: anonymity, remoteness of the protagonist, relative inexpensiveness, absence of necessity to use explosives and suicidal acts, a lot of publicity in the media. However, it is also characterized with downsides: due to the system’s complexity it is difficult to manage the attack and achieve the desired harm directly to people, the act does not become as dramatic and emotional as it happens when using other means. Cyberterrorism is also characterized by the following feature: new information technologies quite often become an instrument of a broader terrorist operation.

Scholars contend that cyberterrorism represent an existential threat, namely as terrorism planned, committed or coordinated in cyberspace, i.e. the latest advances in science and technology in the field of new information technologies are used in terrorist actions (Kondratiev et al., 2004).

Legislative gaps in the counter-cyberterrorism sphere in Ukraine and the ways to overcome them

Cyberterrorism is clearly identified by the writers of this paper as a threat to cyber security. According to *V. P. Shelomentsev*, special entities of cyber security are government agencies which along with general functions are authorized to fight with cybercrime and cyberterrorism, as well as to ensure cyber protection of the national critical infrastructure facilities. Such entities include as follows: The Ministry of Internal Affairs of Ukraine; Security Service of Ukraine; State Service for Special Communications and Information Protection of Ukraine; Ministry of Justice of Ukraine; Prosecutor General's Office of Ukraine (Shelomentsev, 2012).

However, the collision is as follows.

First and foremost, the concept of «cyberterrorism» is missing both in the basic Law of Ukraine «On Counter Terrorism» (Law No. 638-IV, 2003) and in the Concept of Combating Terrorism (Decree No. 230/2013, 2013). That is, the concept of cyberterrorism is missing in the key and fundamental NPAs. That is, de jure, there is no such phenomenon as cyberterrorism.

Second, according to the Law of Ukraine «On Basic Principles of Cyber Security of Ukraine», *cyberterrorism* is a terrorist activity carried out in cyberspace or using cyberspace (Law No. 2163-VIII, 2017).

That is, the generic concept is *«terrorist activity»*, not *«terrorism»*. This is also rather inconsistent given the construction of both the concept itself and the substantive features that distinguish the actual «terrorism» from a pure «terrorist activity».

Third, at the same time, in accordance with the Law of Ukraine «On Counter Terrorism», «*terrorist activity* is an activity that comprise: planning, organization, preparation and implementation of terrorist acts; incitement to commit terrorist acts, violence against individuals or organizations, material facilities destruction for terrorist purposes; illegal armed formations, criminal groups (criminal organizations), organized criminal groups organization to commit terrorist acts as well as participation in such acts; recruitment, arming, training and use of terrorists; terrorist ideology propaganda and dissemination; financing of knowingly terrorist groups (organizations) or other kinds of their support» (Law No. 638-IV, 2003).

Meanshile, no paragraph states that cyberterrorism is a form of terrorist activity. Similarly, in the Art.1 of this Law we will not find any indication that cyberterrorism is the sub-type of terrorism. Thus, purely formally, cyberterrorism as a phenomenon is not legitimized; it does not exist in the legal space, thus none of the entities of the counter-terrorism system has the competence for counter cyberterrorism efforts.

In order to correct this error, it is necessary to introduce appropriate modifications to the Law of Ukraine «On Counter Terrorism», adding paragraph 4 of Art. 1 (Law No. 638-IV, 2003), which defines the concept of terrorist activity, the sentence «financing of knowingly terrorist groups (organizations) or other kinds of their support» shall be added through a semicolon with the following paragraph: *«planning, organization, preparation and implementation of cyberterrorism»*.

In view of the above stated the authors of the research are convinced that the term *«cyberterrorism»* is a synthesis of the concepts of *«cyberspace»* and *«terrorist activity»* and until now it is the dynamic polemic in the academic circles on if the first is just acts of terrorism implementation in the new space or it is fundamentally new phenomenon that has new methods, means and tools.

Definitions of *information terrorism* or *cyberterrorism* can be found both in international legal instruments and draft conventions, as well as in researches done by the experts on this issue. One of the characteristic features of the definitions of information terrorism is that the vast majority of them mention one aspect of information security only, namely the aspect related to date processing means, which narrows the concept of information terrorism, thereby limiting legal regulation sphere, which does not contribute to efficient cooperation of states in their counter information terrorism efforts. *«Cyberterrorism»* is an illegal act committed in order to achieve negative consequences, such as obtaining material benefits or threatening the information security of the state. Cyberterrorism takes place in cyberspace (Diorditsa, 2018).

Prior to cyberterrorism changes from a «potential» threat to a «real» threat, preventive measures should be taken to prevent its formation. The basis for the fight against cyberterrorism is the creation of an effective system of measures to prevent, detect and stop this type of crime (Topchiy, 2015).

Thus, strange as it may appear, at the moment of writing this paper (February 2021) Ukraine has not developed laws and regulations governing public relations in the field of cyberterrorism. However, the main weapon in fighting with this threat is the legislation itself, which needs further improvement.

If one looks at the international legal acts in this area, the first and major instrument that deals with the fight against cybercrime is the European Convention of 2001. This document is focused on implementation of the general policy in the criminal law issues, the aim of which is to protect society from cyberterrorism by adopting the prerequisite legislative acts, as well as by extending international cooperation. There is not even such kind of a crime as cyberterrorism in Ukrainian law. Therefore, the most effective direction to solve the complex issue of counter-cybercrime efforts in our time is the international cooperation of the law enforcement agencies in the information security field based on the national and international legislation harmonization.

The UN Global Counter-Terrorism Strategy and the European Union Counter-Terrorism Strategy are also fundamental documents at the international level.

Cyberterrorism is aimed at penetrating the information and telecommunications system, intercepting control, network data exchange means suppression along with the other destructive actions. The danger of this type of information terrorism is that it has not any national borders, and it is still quite troublesome to detect a terrorist in the information space, as hackers are performing terrorist activities through fictitious computers makes it challenging to identify them and find out their location.

For the time being, cyberterrorism is one of the most dangerous types of crime. Cyberattacks can cause significant damage locally, nationally and even internationally. After all, external cyberattacks can pursue much more ambitious goals than passive data collection, and cyberterrorism may focus on the monetary and secret information, space systems control hardware, nuclear power plants control and monitoring systems, military complexes supervision equipment, major computer nodes, etc (Iatsyk, 2014).

Today, there are two bid agencies ready to take the lead in the fight against cyberterrorism at the international level. This is the OSCE Counter-Terrorism Unit, a UN-sponsored organization, and Interpol. In addition, the European Cybercrime Center started its operations in the European Union. EU member states and European institutions intend to support the European Cybercrime Center to create operational and analytical investigative capacities and to cooperate with international partners.

Conclusions

Having analyzed and researched the development of cybercrime on the territory of Ukraine, authors cannot state with confidence that the concept of the state is focused on integrating efforts to combat this phenomenon. The legal document that regulates relations in this sphere in Ukraine is the Doctrine of Information Security of Ukraine, one of the key issues of which is technogenic security provision, including in the field of its information aspects and the fight against technological terrorism.

However, it is not an effective regulator in its field. In addition, the Law of Ukraine «On the Principles of the State Information Policy» has not been adopted yet, and the adopted Law of Ukraine «On the Basic Principles of Cyber Security of Ukraine» (Law No. 2163-VIII, 2017) has numerous significant detriments that narrow down its valuability as regulator of public relations. Moreover, in Ukraine only table talks on the National Cyber Security System formation are still going on, however it was not created and established any specific programs for this task implementation in the state cyber security policy context containing the definitions of the aim, time, place, tasks and responsibilities.

In similar fashion, *Cyber Command* has not been created in Ukraine, notwithstanding it is long existing in a number of the developed countries, to respond in fast manner the challenges in the stat’s information security area. In conclusion, it should be noted that the pending issue of combating acts of cyberterrorism is a complex problem that requires an interdisciplinary approach to its comprehensive solution.

Bibliographic references

Berner, S. (2003). Cyber-Terrorism: Reality or Paranoia? South African Journal of Information Management, 5(1), pp. 1-4. DOI: 10.4102/sajim.v5i1.208

Boeckmann, R. & Turpin-Petrosino, C. (2002). Understanding the Harm of Hate Crime. Journal of Social Issues, 58(2), pp. 207-225. DOI: 10.1111/1540-4560.00257

Budhijanto, D. (2019). The Virtual Jurisdiction to Combating Cyberterrorism in Indonesia. Central European Journal of International and Security Studies. Issue 12(4), pp. 61–80. Retrieved from https://www.researchgate.net/publication/332318760_The_Virtual_Jurisdiction_to_Combating_Cyberterrorism_in_Indonesia

Burayachok, V.L., Tolubko, V.B., Khoroshko, V. O. & Tolyupa S.V. (2015). Information security and cyber security: sociotechnical aspect. Kyiv: DUT, 288 p. Retrieved from http://www.dut.edu.ua/uploads/l_1209_69915296.pdf

Cavelty, M.D. (2007). Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. Journal of Information Technology and Politics, 4(1), https://doi.org/10.1300/J516v04n01_03

Cavelty, M.D. (2018). Cybersecurity Research Meets Science and Technology Studies. Politics and Governance, 6(2), pp. 22-30. DOI: https://doi.org/10.17645/pag.v6i2.1385

Cohen-Almagor, R. (2005). Media Coverage of Acts of Terrorism: Troubling Episodes and Suggested Guidelines. Canadian Journal of Communication, 30(3), pp.383-409.

Cyber Policy Center (2021). Clubhouse in China: Is the data safe? Stanford Internet Observatory. Retrieved from https://cyber.fsi.stanford.edu/io/news/clubhouse-china (accessed February 12, 2021).

Decree of the President of Ukraine No. 230/2013. Concept of Combating Terrorism. Verkhovna Rada of Ukraine, April 25, 2013. Retrieved from https://zakon.rada.gov.ua/laws/show/230/2013#Text

Diorditsa, I.V. (2018). Cyber security policy of Ukraine: status and priority areas of implementation: monograph. Zaporizhzhya: Helvetica Publishing House, 548 p.

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR) relevant theory? International Political Science Review, 27(3), pp. 221–244. https://doi.org/10.1177/0192512106064462

Foros, G.V., Foros, A.V. (2010). Information terrorism as a threat to the national security of Ukraine. Constitutional state, No. 12, pp. 256-261.

Furnell, S.M. and Warren, M.J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium? Computers and Security, 18(1), pp. 28-34. https://doi.org/10.1016/S0167-4048(99)80006-6

Hryzchuk, V.K. (2011). Terrorism: theoretic and applied aspects. Lviv: Lviv DUVS, 328 p.

Iatsyk, T.P. (2014). Specific features of the information terrorism as one of the methods of information war. HScientific bulletin of the National University of the State Tax Service of Ukraine (economics, jurisprudence), No. 2, pp. 55–60.

Ieroshenko, O. (2012). Explanatory Dictionary of the Modern Ukrainian language. Donetsk: Gloriya Trade, p. 282.

Kondratiev, Ia.Iu, et al. (2004). Detection and investigation of crimes committed in information technology field. Kyiv: Palyvoda A. V., 144 p.

Kubyshkin, O.V. (2002). International-legal issues of the state information security arrangements (Doctoral thesis). Moscow State Law Academy, Moscow. Retrieved from http://pravolib.pp.ua/informatsionnyiy-terrorizm-15103.html

Lux, M.Y. (2018). Defining cyberterrorism. Revista Chilena de Derecho y Tecnología, 7(2), pp. 5-25. http://dx.doi.org/10.5354/0719-2584.2018.51028

Law of Ukraine No. 638-IV. On Counter Terrorism. Verkhovna Rada of Ukraine, March 20, 2003. Retrieved from https://zakon.rada.gov.ua/laws/show/638-15#Text

Law of Ukraine No. 2163-VIII. On Basic Principles of Cyber Security of Ukraine. Verkhovna Rada of Ukraine, October 5, 2017. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text

Law of Ukraine No. 2289-IV. On Amendments to the Criminal and Criminal and Procedure Codes of Ukraine. Verkhovna Rada of Ukraine, December 23, 2004. Retrieved from https://zakon.rada.gov.ua/laws/show/2289-15#Text

Lee, J. & Macdonald, S. (2015). What Is Cyberterrorism? Findings from a Survey of Researchers. Terrorism and Political Violence, 27(4). DOI: 10.1080/09546553.2013.847827

Lee, Jarvis, Macdonald, S. & Nouri, L. (2014). The Cyberterrorism Threat: Findings from a Survey of Researchers. Studies in Conflict & Terrorism, 37(1), pp. 68-90, DOI: 10.1080/1057610X.2014.853603

Lewis, J.A (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. Retrieved from https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Lipkan, V. (2008). Administrative law basis of ensuring national security of Ukraine. (Doctoral thesis). Kyiv National University of Internal Affairs, Kyiv. Retrieved from https://goal-int.org/avtoreferat-2/

Lipkan, V.A., Maksimenko Yu.E., Zhelikhovsky V.M. (2006). Information Security of Ukraine in the Conditions of European Integration. Kyiv: CST, 280 p. Retrieved from http://www.dut.edu.ua/uploads/l_1350_59375830.pdf

Lipkan, V., Baskakov V. (2011). Protection of information with limited access in the fight against organized crime. Fight against organized crime and corruption (theory and practice), Vol. 24, pp. 263-269. Retrieved from http://nbuv.gov.ua/UJRN/boz_2011_24_32

Makarenko, Ie. A. (2011). International cooperation in the field of information security: regional context. Actual problems of international relations, 24(1), pp. 51-62. Retrieved from http://journals.iir.kiev.ua/index.php/apmv/article/view/2116/1879

Mason, O.J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: The Cyber-Paranoia and Fear Scale. Frontiers in Psychology. https://doi.org/10.3389/fpsyg.2014.01298

Ministry of Foreign Affairs of Japan (2000). Okinawa Charter on Global Information Society. G8 Kyushu-Okinawa Summit Meeting 2000, Kyushu-Okinawa Japan. Retrieved from https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html

Pašagić, A. (2020). Failed States and Terrorism: Justifiability of Transnational Interventions from a Counterterrorism Perspective. Perspectives on Terrorism, 14(3), pp. 19-28. Retrieved from https://www.jstor.org/stable/26918297

Poteriakhina, I.S. (March, 2012). Role of cyberterrorism in the current international relations. In K. Balabanov of the President of the Conference, Trends in the development of the modern system of international relations and the world political process. Conference led by Mariupol State University, Mariupol, Ukraine. pp. 37-40. Retrieved from http://repository.mdu.in.ua/jspui/bitstream/123456789/119/1/Tend_rozv_such_systemy_MV_2012.pdf

Shelomentsev, V.P. (2012). The essence of organizational support of the cyber security system of Ukraine and the ways to improve it. Fight against organized crime and corruption (theory and practice), No. 2(28), pp. 299–309.

Shyrokova-Murarash, O. G., & Akchurin, Yu. R. (2011). Cybercrime and cyberterrorism as the threats to the global information security: international and legal aspect. Information and law, No. 1, pp. 76–81.

Sokur, S. (2010). Forming common EU security and defense policy in the context of fighting against modern cyberterrorism. Viche. No. 10, pp. 24-27. Retrieved from http://nbuv.gov.ua/UJRN/viche_2010_10_10

Tafoya, W. L. (2011). Cyber Terror. FBI Law Enforcement Bulletin. Retrieved from https://leb.fbi.gov/articles/featured-articles/cyber-terror

Topchiy, V.V. (2015). Cyber terrorism in Ukraine: concept and prevention by criminal and legal and criminological means. Scientific bulletin of Kherson State University. Series: Legal science, Issue 6, pp. 65-68. Retrieved from http://nbuv.gov.ua/UJRN/Nvkhdu_jur_2015_6%283%29__16

Vilić, V.M. (2017). Dark web, cyber terrorisam and cyber warfare: dark side of the cyberspace. Balkan Social Science Review, Vol. 10, pp. 7-25. Retrieved from https://js.ugd.edu.mk/index.php/BSSR/article/view/1939/1708

Weimann, G. (2004). Cyberterrorism: How Real is the Threat? United States Institute of Peace. Retrieved from https://www.usip.org/sites/default/files/sr119.pdf (accessed 02 March 2021), p. 6.

Zelenkov, M.Y., Ponomarev, V.G., Gusev, V.V., Andreev, A.N., & Makarov, O.N. (2020). Identification of Advertising Trends in the Mass Media and On the Internet Used by Modern Terrorism. Cuestiones Políticas, 37(65), pp. 382-398. DOI: https://doi.org/10.46398/cuestpol.3865.26

Zulhuda, S. (2020). The threat of cyberterrorism and the applicability of the convention of cybercrime. At Tahalof (Terrorism in International Law), 3, pp. 20-23. Retrieved from http://irep.iium.edu.my/80983/1/At-Tahalof%20Issue%203%20%28May%202020%29%20English.pdf