Cristina EJOVA
Moldova State University, Republic of Moldova

ANALYSIS OF THE CONCEPT OF CYBERTERRORISM IN THE CONTEXT OF POLITICAL SCIENCE

Abstract:	*This paper examines the concept of cyberterrorism through the lens of political science, focusing on its origins, development, and impact on global security. With the exponential growth of information technology, cyberterrorism has emerged as a significant threat, utilizing advanced technological means to destabilize political and social frameworks. The rapid increase in internet access has introduced new opportunities for both communication and crime, including the use of digital platforms for extremist and terrorist activities.* *The study emphasizes the complex methodologies required for analyzing cyberterrorism, including systemic, institutional, and comparative approaches, each contributing to a nuanced understanding of this phenomenon. Based on a systemic approach, the specifics of various definitions of the phenomenon of "cyberterrorism" will be revealed. It is argued that modern cyberterrorism, aimed at creating threats to international and national security, serves as one of the effective tools for achieving political goals on the global stage. Utilizing theories such as the information society and network society, the article underscores the importance of international cooperation in combating cyberterrorism.*
Keywords:	**Cyberterrorism; cyberspace; cyber-attack; Internet; information society**
Contact details of the authors:	E-mail: cristina.ejova@usm.md
Institutional affiliation of the authors:	**Department of International Relations, Faculty of International Relations Political and Administrative Sciences, Moldova State University, Republic of Moldova**
Institutions address:	Moldova State University, 60 A. Mateevici Str., Chișinău, http://usm.md

Introduction

The modernization of society and the development of information technologies have led to the widespread use of the Internet worldwide, giving rise to one of the most dangerous forms of cybercrime – cyberterrorism, which utilizes the latest advancements in science and technology. The twenty-first century can confidently be called the century of information technologies, due to their constant development and integration into our lives. The emergence of global informatization has resulted in the creation of a unified information space – the World Wide Web and new ICT tools. More than 66% of the world's population uses the Internet, and according to the latest data, the total number of Internet users globally amounts to 5.35 billion. Over the past 12 months, the Internet audience has grown by 1.8% (97 million new users since the beginning of 2023)[1]. However, the rapid expansion of the digital realm has created opportunities for exploitation by extremist and terrorist

[1] *Digital 2024: Global Overview Report*, https://indd.adobe.com/view/8892459e-f0f4-4cfd-bf47-f5da5728a5b5 (02.04.2023)

organizations, which use these platforms to disseminate propaganda, recruit members, and even operational planning.

A prominent illustration of this phenomenon is the online presence and activities of the terrorist group "Islamic State of Iraq and the Levant" (ISIS). In 2014, ISIS disseminated a documentary titled *The Clanging of the Swords* via global online platforms, serving as a potent instrument of psychological propaganda. The film depicted brutal scenes of ISIS armed forces' combat actions against the government troops of Syria and Iraq, bloody massacres of civilians, and the families of military personnel. This content was created to intimidate and spread extremist ideology.

The group also capitalized on the video game industry by developing a modified version of the popular game Grand Theft Auto (GTA), named GTA–ISIS: The Jihad Simulator, which integrated their ideology. Social media has proven to be another essential tool for ISIS. The group used part of the technological infrastructure of global social networks to actively propagate on behalf of the "Islamic State" on platforms as "VKontakte" and others. These platforms not only served as channels for content dissemination but also played a key role in the recruitment of new members.

The dual nature of the development of information and communication technologies underscores the urgent need for the development of comprehensive strategies to monitor, regulate, and counter the misuse of digital spaces by such organizations.

The influence of global networks on the socio-political development of society is multifaceted and contradictory. On the one hand, they contribute to the development of human potential through computer games, educational and entertainment programs, interactive television, and electronic media. Global networks also impact the electoral behavior of political actors, the organization and conduct of election campaigns, mechanisms of communication between the government and society, as well as the presentation and advocacy of political actors' interests. On the other hand, the rapid development of the information and communication sphere has led to the emergence of new types of crimes – computer crime and cyberterrorism. Some notable examples have been recorded in the past years.

In recent years, cyberattacks have an alarming increase on a global scale. According to a report published in 2024 by Check Point Research, the number of cyberattacks worldwide has risen by approximately 30% over the past two years, highlighting a dangerous trend in the advanced use of technology by malicious entities. This situation not only amplifies risks but also increases the probability that terrorist groups and organizations will utilize cutting-edge technologies to commit actions bearing the hallmark of terrorism or to achieve terrorist objectives[1]. A relevant example is the cyberattacks of 2024. In January 2024, while Sweden was preparing to join NATO, a ransomware attack was launched on the governmental digital service. The attack, carried out by a Russian hacker group, disrupted the functioning of 120 government offices[2]. Just six months later, a Microsoft Windows update led to a global IT outage, interrupting the operations of airlines and hospitals[3].

Although the incident was caused by a malfunctioning software update, it exposed users, both individuals and private companies, to additional planned attacks. Around 8.5 million machines were affected, resulting in a loss of $5.4 billion for Fortune 500 companies[4]. In 2021, the Center for Strategic and International Studies (CSIS) identified 118 cyberattacks that could be classified as acts of cyberterrorism. These attacks targeted government institutions, major information technology

[1] Check Point, *Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks,* July 2024, https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/ (26.11.2024)

[2] Center for Strategic and International Studies, *Significant Cyber Incidents* https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (26.11.2024)

[3] *Idem*

[4] *Idem*

companies, and defense industry enterprises. Among the incidents were cyberattacks on major critical infrastructure facilities such as the water supply system in Oldsmar, Florida; Poland's National Atomic Energy Agency; Poland's Ministry of Health, and several others. Since 2023 the Center has recorded over 800 cases, underlying the severity of the situation and the vulnerability of governments and individuals in the digital sphere[1].

The activities of cyberterrorists in virtual space can harm thousands of network users, not only individuals but entire states. Global informatization processes and the development of information technologies have led to the creation of a new platform for criminal activity, which requires new approaches to ensuring security.

Methodological approaches to research

The study of cyberterrorism presents a complex scientific challenge due to the multifaceted nature of this phenomenon, which encompasses political, social, psychological, and technical aspects. This issue cannot be confined to a single definition and requires an interdisciplinary approach, involving political science, sociology, psychology, law, information technology, and other fields. The rapid development of information and communication technologies adds complexity to the study of cyberterrorism, as this process impacts virtually all areas of modern society. The main methodological approaches in cyberterrorism research include *systemic, institutional, structural-functional*, and *comparative approaches*. Scientific investigation of relevant topics is also carried out through the application of research theories such as information society theory and network society theory.

The systemic approach in researching the phenomenon of cyberterrorism involves viewing it as an integrated and complex issue, which requires recognizing the essential elements of international cooperation for effectively preventing and countering cyber threats. Since cyberterrorism transcends national borders and is characterized by global technological interdependence, its effective counteraction is only possible through strong international collaboration. The systemic approach allows for a deeper understanding of the interactions among actors, infrastructures, and cybersecurity policies, enabling the development of common defense and prevention strategies that provide effective protection against cross-border cyberattacks.

The institutional approach allows for an assessment of how government and specialized institutions (such as the presidency, parliament, and security services) respond to cyberterrorism threats. This study focuses on the structure, functions, and interactions between various organizations to develop coordinated measures to counter cyber threats. The institutional approach also includes the study of other countries' experiences and practices in cybersecurity, enabling consideration of global trends and adaptation of effective international strategies to the national context.

The author has also applied *structural-functional analysis* as methodological support. The method of structural-functional analysis is aimed at solving issues related to maintaining stability, functioning, and viability of the system. The structural component involves identifying the main elements of the system and stable connections between them. In turn, the functional component analyzes the mechanisms of interaction between these elements and determines how the system interacts with the external environment. Understanding the internal interconnections and interactions between system components allows for identifying the conditions necessary for its operability and the influence of external factors on its functioning. Applied to cyberterrorism, this method enables the formation of a counteraction system structure that includes subsystems such as institutional, regulatory-legal, organizational-functional, communicative, human resources, and cultural. This

[1] Center for Strategic and International Studies, *Significant Cyber Events List*, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-11/241114_Significant_Cyber_Events.pdf?VersionId=x077LxbEUZ9.EQb8yEUMcTa5ebhzQHQe (26.11.2024)

approach facilitates a comprehensive analysis and the development of policies to counter cyber threats.

The comparative method in analyzing the phenomenon of cyberterrorism offers a complex perspective, allowing for the comparison of approaches and contributions by Western and Russian authors. This method helps identify differences and similarities in the definition and understanding of the phenomenon, prevention and counteraction strategies, as well as the role of the state and international institutions. Studies by Western authors tend to focus on the technological and critical infrastructure aspects of cyberterrorism, emphasizing the importance of international cooperation and rapid adaptation to new cyber threats. In contrast, Russian authors often emphasize the role of national sovereignty and the need for strict internal regulation in managing cyber risks.

Comparing these perspectives enables a clearer understanding of the priorities and challenges each approach faces. For instance, Western sources extensively explore the development of public policies and public-private partnerships in cybersecurity, whereas Russian authors focus on the direct involvement of the state and government control measures. Thus, the comparative method provides not only a diversity of views on the phenomenon, but also potential solutions tailored to the specific political and social context of each region.

Information society theory. Information society theory, which emerged as part of the post-industrial society concept, emphasizes changes in a society where the production, distribution, and consumption of information take center stage. In such a system, the role of cybersecurity and the protection of information infrastructures increases. Information technologies, on the one hand, facilitate improvements in public policy and crisis management; on the other hand, they can generate new threats, such as cyberterrorism.

Network society theory. Network society theory explains how global social changes in the last decades of the 20th century led to the formation of a new social structure based on network interaction. At the core of this theory are information and communication technologies, which facilitate the active reproduction of knowledge. As the role of global networks (such as the internet, political, and terrorist networks) grows, state structures and power relations also undergo changes, replacing traditional hierarchies with network forms of interaction and decentralized power distribution.

The network society significantly influences socio-political development by fostering constructive interaction between state institutions and society. However, it also introduces new threats, such as cyberterrorism. The theory of the network society provides a framework for analyzing the conditions that facilitate the spread of cyberterrorism through global networks. Moreover, it aids in devising effective countermeasures tailored to the complexities of interconnected digital structures[1].

Definition and specificity of cyberterrorism

The term “cyberterrorism” was first used in 1980 by B. Collin, a specialist at the Institute for Security and Intelligence in California[2]. He used this term to denote the potential for terrorist attacks in cyberspace. At that time, the precursor to the Internet—the ARPANET network of the U.S. Department of Defense's Advanced Research Projects Agency—connected only a few dozen computers within one country. However, the researcher was certain that, although cyber networks would eventually be embraced by terrorists, this development would not happen before the first decade of the 21st century[3]. In the 1980s, this term had not yet materialized and was used as a

[1] Eliot Che, *Securing a Network Society: Cyber-Terrorism, International Cooperation, and Transnational Surveillance,* ”Research Paper”, No. 113, Research Institute for European and American Studies (RIEAS), Athens, September 2007, pp. 25-26, https://rieas.gr/images/RIEAS113ELIOTCHE.pdf (03.12.2024)
[2] Barry Collin, *The Future of Cyber Terrorism*, “Crime & Justice International”, Vol. 13, No. 2, March 1997, p. 16
[3] *Ibidem*, p.18

projected development for the near future. In 1997, FBI special agent Mark Pollitt defined this type of terrorism as "politically motivated attacks on information, computer systems, computer programs, and data, expressed through violence against civilian targets by subnational groups or clandestine agents"[1].

To define the term cyberterrorism, it is also necessary to define the terms terrorism and cyberspace. Cyberspace is a global domain of interconnected and interdependent networks where data is processed, transferred, and stored in machine-readable formats. It encompasses not only a virtual level, including digital systems and programs, but also a physical infrastructure and a human domain that reflects user activities and interactions. This multifaceted space plays a critical role in technological and sociopolitical processes, shaping and being shaped by global dynamics[2].

Terrorism is a complex socio-political phenomenon that represents an act of illegal violence or a threat of using it, deliberately committed by individuals or a group of persons to achieve a political or ideological goal that can be national, transnational, or international in nature. Another key element of terrorism lies in its ability to instill fear in society and intimidate the population to achieve specific political aims. At the same time, the causes of terrorism may be economic, political, religious, or territorial. Contemporary terrorism is marked by the following traits: a complete lack of control by state structures; a hybrid nature, involving a combination of criminal motives and terrorist ideology; rapid transformation; the expansion of the technical capabilities of destructive weapons; increased scope and geographic spread; and strong financial backing[3].

One of the first groups to use the internet for illicit purposes is the "Tamil Tigers" who, in 1998, bombarded Sri Lankan government offices with emails for two weeks, referring to themselves as the "Black Internet Tigers". Around the same time, "Aum Shinrikyo" (as discovered during searches of the organization's headquarters) was working on the possibility of intercepting control over nuclear facilities[4].

The study of cyberterrorism as a scientific discipline has several unique characteristics. First, it is interdisciplinary, encompassing research in political, legal, and technical fields. Second, it is practically oriented, directly addressing challenges related to information security. These factors contribute to a wide range of theoretical approaches applied to understanding this phenomenon.

The international community has not yet developed a unified definition of "cyberterrorism", which makes it difficult to develop effective measures to combat this type of crime. Specialists in international relations and law, as well as representatives of international organizations, face problems in formulating this concept, as well as in distinguishing between the term's "cybercrime" and "cyberterrorism". Unlike cybercriminals, the main goal of terrorist organizations is "inciting international and social tension, stirring up ethnic and religious hatred and enmity, promoting extremist ideology, attracting new supporters through informational influence on individual, group and public consciousness", as well as using means of destructive impact (cyber weapons) on critical information infrastructure objects. However, according to experts, "to date, there has been no

[1] Mark M. Pollitt, *Cyberterrorism: Fact or Fancy?,* "Computer Fraud and Security", February 1998, pp. 8–10

[2] Nick Ebner, *Cyber Space, Cyber Attack and Cyber Weapons A Contribution to the Terminology*, "Institute for Peace Research and Security Policy at the University of Hamburg", Hamburg, October 2015, p. 3, https://epub.sub.uni-hamburg.de/epub/volltexte/2018/80797/pdf/IFAR2_FactSheet7.pdf (02.12.2024)

[3] Cristina Ejova, *Unele abordări conceptuale ale terorismului, "*Studia Universitatis Moldaviae. Științe Sociale"*,* No. 3, 2023, pp. 252-253, https://social.studiamsu.md/wp-content/uploads/2023/05/31_C_Ejova.pdf (15.10.2024)

[4] Galina Kuleshova, Elena Kapitonova, Georgy Romanovsky, *Pravovye osnovy protivodejstviya kiberterrorizmu v rossii i za rubezhom s pozicii obshchestvenno- politicheskogo izmereniya*, "Russian Journal of Criminology", Vol. 14, No. 1, 2020, p. 157, https://cyberleninka.ru/article/n/pravovye-osnovy-protivodeystviya-kiberterrorizmu-v-rossii-i-za-rubezhom-s-pozitsii-obschestvenno-politicheskogo-izmereniya (2.11.2024)

recorded large-scale use of malicious software by terrorist organizations aimed at disrupting the operation of critical information infrastructure"[1].

The lack of a universal definition of terrorism complicates the characterization of cyberterrorism without reference to traditional forms of terrorism. In this regard, let us turn to the opinions of scholars in the field of political science.

In 2000, Professor of Computer Science at Georgetown University, Dorothy Denning, one of the most authoritative experts in cybersecurity, categorized terrorists' activities on the Internet into three groups: activity, hacking, and cyberterrorism. By "activity", she refers to the simple use of computer technologies for the purposes of propaganda, fundraising, and attracting new followers. In this context, cyberspace serves as a means that facilitates the unification of terrorists and the recruitment of new members into terrorist organizations. The online capabilities for collecting donations are vast, ranging from simple transfers of funds through methods indicated on websites.

Hacking refers to illegal attacks on computer networks, secret databases, and websites to obtain information or steal money.

Cyberterrorism is defined by the researcher as "illegal attacks or threats of attacks on computers, networks, and the information stored within them, aimed at intimidating or coercing governments or citizens into taking certain actions for political or social purposes"[2]. The researcher also noted that while cyberterrorism is similar in its implementation methods to hacking, it represents, according to Danning, a distinctly different type of computer attack that involves causing significant damage to critical infrastructure using information technologies[3].

We agree with Danning's position; her classification of terrorist activities in cyberspace into three groups allows for a clearer understanding of the distinctions between types of cyberattacks. It is important to emphasize that it is the political motive and the intent to exert pressure on the government that differentiates cyberterrorism from other forms of illegal activity in the network. This definition helps to highlight the destructive potential of cyberterrorism.

Also, in the 2000s, the German scholar K. Hirschmann, in his work "The Changing Face of Terrorism" defined cyberterrorism as a premeditated, politically motivated attack on information and cyberspace for terrorist purposes, meaning operations aimed at breaking into computer systems, computer programs, and their processing, which take the form of violence against neutral objects by subnational groups or individuals acting clandestinely[4]. Hirschmann, in turn, views cyberterrorism as a consciously planned political attack, where the concealment of actions holds particular significance. Thus, his approach enhances the understanding that cyberterrorist attacks are aimed not merely at disrupting systems but also at destabilizing with a political objective. Researchers M. J. Devost, B. X. Houghton, and N. A. Pollard define cyber-terrorism as:

(1) the combination of criminal use of information systems through fraud or abuse with physical violence characteristic of terrorism; and

---

[1] UN General Assembly, *Resolution A/54/49: Developments in the Field of Information and Telecommunications in the Context of International Security,* December 1, 1999, https://documents.un.org/doc/undoc/gen/n99/777/13/pdf/n9977713.pdf (02.11.2024)

[2] Dorothy E. Denning, *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, May 23, 2000, https://irp.fas.org/congress/2000_hr/00-05-23denning.htm (02.11.2024)

[3] Dorothy E. Denning, *Is Cyber Terror next*?, "Social Science Research Council", https://items.ssrc.org/after-september-11/is-cyber-terror-next/ (02.11.2024)

[4] Kai Hirschmann, *The changing face of terrorism*, „International Politics", No. 3, 2000, p. 308, https://library.fes.de/pdf-files/ipg/ipg-2000-3/arthirschmann.pdf (02.11.2024)

(2) the intentional misuse of digital information systems, networks, or components of those systems or networks for purposes that facilitate the execution of terrorist operations or acts[1].

American researcher K. Wilson defines cyber-terrorism as the use of computers as a weapon or target by politically motivated international or transnational groups, or clandestine agents, who threaten or inflict violence and instill fear to influence or coerce the government to change its policies[2].

According to Dutch researcher Ruben Tuitel, cyber-terrorism is the use of cyberspace by non-state actors to disrupt the functioning of computer systems, instill a sense of fear, or cause physical harm, and indirectly, health damage, or create disruptions that seriously threaten the reputation of the victim, carried out for political, ideological, or religious purposes[3]. We agree with this opinion, as it highlights the multifaceted nature of cyberterrorism and the importance of its political, ideological, or religious orientation.

A well-known expert on cyberterrorism, Professor Gabriel Weiman from the Faculty of Communications at the University of Haifa, defines cyber-terrorism as a specific intersection of cyberspace and terrorism, including illegal cyberattacks or threats of such attacks on information networks aimed at intimidating or coercing the government or its people to achieve political goals. According to Weiman, such classification is only possible if the outcomes lead to serious consequences that instill fear in the population, and attacks on critical infrastructure should be classified based on the damage caused. He identifies several features of cyber-terrorism at the present stage: firstly, cyberattacks are significantly cheaper compared to traditional terrorist methods; secondly, cyberterrorism provides terrorists with a high level of anonymity, complicating security services' efforts to identify them; the global network offers a wide range of targets, allowing effective attacks to be carried out remotely, thereby reducing the need for physical preparation and lowering risks for the perpetrators; additionally, digital attacks can reach a substantial number of users, capturing media attention and amplifying the impact that terrorists aim to achieve[4].

Professor Gabriel Weiman also notes that while the threat of cyberterrorism may be exaggerated, it cannot be ignored [5].

Weiman rightly emphasizes the uniqueness of cyberterrorism, highlighting its specific characteristics, such as anonymity and the remote nature of attacks. Indeed, the potential for covert influence achieved in cyberspace makes cyber-terrorism a powerful tool for political pressure, as evidenced by extensive media coverage of such attacks. At the same time, his warning about the possible exaggeration of the threat of cyberterrorism points out the need for a balanced approach in assessing cyberattacks on critical infrastructure and in developing strategies for their prevention.

Jerome Orji, an expert in cybersecurity and its regulatory framework, a researcher at the African Centre for Cyberlaw and Cybercrime Prevention (ACCP) in Kampala, Uganda, categorizes cyberterrorism as a terrorist attack against or through computers and network infrastructures aimed at disrupting vital sectors and achieving terrorist objectives: loss of life, panic, economic collapse, or intimidation to influence government policy[6].

---

[1] Tat'yana Tropina, *Kiberprestupnost' i kiberterrorizm: pogovorim o ponyatijnom apparate*, in *Informacionnye Tekhnologii i Bezopasnost'". Sbornik nauchnyh trudov mezhdunarodnoj konferencii*, Nacional'naya Akademiya Nauk Ukrainy, Kyiv, 2003, pp. 177 – 178

[2] Clay Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues*, October 2003, https://apps.dtic.mil/sti/pdfs/ADA421056.pdf (02.11.2024)

[3] Ruben Tuitel, *Defining cyberterrorism*, "PerConcordia. Journal of European Security and Defense Issues", Vol. 7, No. 2, 2016, p. 12, https://perconcordiam.com/perCon_V7N2_ENG.pdf (02.11.2024)

[4] Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation*, New York, 2015, p. 25

[5] Gabriel Weimann, *Cyberterrorism: How Real Is the Threat? Special Report 119*, United States Institute of Peace, Washington, DC, 2004, https://www.usip.org/sites/default/files/sr119.pdf (02.11.2024)

[6] Uchenna Jerome Orji, *Deterring cyberterrorism in the global information society: A case for the collective responsibility of states*, "Defense Against Terrorism Review", Ankara, Vol. 6, No. 1, 2014, p. 33

Orji's definition highlights cyberterrorism as a specific form of terrorism aimed at critical infrastructures to create threats, destabilization, and panic. Thus, cyber-terrorist actions take on a distinctly political orientation, emphasizing not only the technical but also the strategic level of impact. Orji's approach emphasizes the flexibility that digital space provides to terrorists seeking to influence government decisions and public sentiment.

The Congressional Research Service of the United States has formulated two main approaches to understanding cyberterrorism:

1. Effect-based approach: Cyberterrorism can be defined as computer-based attacks that generate a level of fear comparable to traditional acts of terrorism, even if these attacks are carried out not by terrorists but by criminals.

2. Intent-based approach: Cyberterrorism is defined as an illegal, politically motivated computer attack intended to intimidate or coerce the government or citizens to achieve further political objectives or to inflict significant damage or serious economic harm[1].

According to the researcher at the Institute of Security and Global Affairs at Leiden University T. Tropina, cyberterrorism aims to intimidate the civilian population and government authorities to achieve criminal objectives. She notes that this manifests through threats of violence, the maintenance of a constant state of fear, coercion into specific actions, and drawing attention to the identity of the cyberterrorist or the organization they represent. We support this perspective, as it highlights the unique transparency of cyberterrorism: cyberattacks are often accompanied by public demands, distinguishing them from other forms of cybercrime[2].

One of the earliest legally established definitions of cyberterrorism is found in the "USA Patriot Act of 2001", enacted by the U.S. Congress following the terrorist attacks of 2001. The concept of "cyberterrorism" in this act includes various qualified forms of hacking and damage to protected computer networks belonging to civilians, legal entities, and government agencies, including harm inflicted on computer systems used by government institutions for organizing national defense or ensuring national security[3]. Later, the issue of countering threats in cyberspace increasingly attracted the attention of the global community.

The United Nations document defines cyberterrorism as the use of information and communication technologies (ICT) to execute terrorist acts, including spreading propaganda, recruitment and radicalization, coordinating attacks, and financing terrorist activities. Additionally, cyberterrorism encompasses targeting critical infrastructure, potentially leading to severe economic, social, and physical repercussions. The document highlights the importance of international collaboration and information exchange to counteract cyber threats and secure cyberspace from terrorist activities. This characterization aligns with current challenges, as terrorist exploitation of the internet complicates monitoring efforts and necessitates new measures to control and protect critical information systems at both national and global levels[4].

An analysis of various definitions of cyberterrorism shows that its primary distinction from other types of crimes lies in its goals, which are akin to those of traditional political terrorism—intimidating or coercing governments or populations into specific political or social actions. In this context, attacks using information technology must result in harm to individuals or significant

---

[1] Prem Mahadevan, *Cybercrime. Threats during the COVID— 2019 Pandemic,* Global Initiative Against Transnational Organized Crime, April 2020, https://globalinitiative.net/wp-content/uplApril020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf (02.11.2024)

[2] Tat'yana Tropina, *Kiberprestupnost'. Ponyatie, sostoyanie, ugolovno-pravovye mery bor'by: monografiya*, Vladivostok, 2009, p. 237

[3] United States Congress, *USA Patriot Act of 2001,* congress.gov/107/plaws/publ56/PLAW-107publ56.htm (02.11.2024)

[4] United Nations Office on Drugs and Crimes, *The Use of the Internet for Terrorist Purposes,* New York, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (02.11.2024)

property damage. Thus, cyberterrorism can be characterized by several key features: the use of technology for attacks, political motivation of the attackers, and the infliction of substantial harm on citizens, organizations, or states.

Features of cyberterrorism as a new kind of terrorist attacks

A cyberattack is a serious threat to humanity, comparable to nuclear, biological, and chemical weapons. Due to its novelty, the extent of this threat is not yet fully recognized or studied. A cyberattack knows no national borders, and a cyberterrorist can equally threaten information systems located almost anywhere on the globe. Detecting and neutralizing a virtual terrorist is extremely challenging due to the minimal traces they leave behind and the unique virtual nature of these traces[1].

Some researchers identify various methods for conducting cyberattacks, including unauthorized access to classified government and military data, banking information, and personal data; causing damage to elements of cyberspace, such as disrupting power grids, creating interference, or introducing viruses to destroy hardware; theft, damage, or destruction of critical information and software through hacking and spreading viruses; disclosure and blackmail through the publication of confidential information; taking control of secured media channels to spread disinformation, demonstrate terrorist strength, or issue demands; and destruction or manipulation of communication lines. A critical concern is the vulnerability of essential infrastructure systems—such as transportation, nuclear power plants, water supply, and energy networks—that are increasingly connected to the Internet[2].

Cyberterrorism should include attempts to disrupt or destroy the functioning of computer systems or the information infrastructure networks of the state or governing bodies. Such criminal acts targeting critical information infrastructure represent a significant threat that could have the most serious consequences for society.

The Maryville University classifies cyberterrorism attacks into three main categories:

Malware: Malicious software refers to programs designed to infiltrate computers and networks without permission, causing damage or disruption with the intent to harm the victim or generate financial profit for the attacker. Common methods for delivering malware include phishing emails, email attachments, harmful advertisements, fake software installation files, and infected USB drives or applications. Various types of malwares include ransomware, which locks or encrypts data for ransom, viruses that trigger harmful actions upon activation, worms that replicate across systems, and spyware that monitors user activity, captures communications, and collects personal information.

Phishing: An attack disguised as an email is designed to deceive the recipient into executing malware that gathers personal data or causes other types of harm. This method is widely used by cyber terrorists and criminals to compromise the devices and networks of their targets. A growing trend in cybercrime involves attackers concentrating on developing the ransomware payload while outsourcing the phishing aspect to a third party, known as an "initial access broker".

Ransomware: Malicious software that locks the victim out of their computer files and restricts access to other resources, only releasing them once a ransom is paid, typically in cryptocurrency like Bitcoin. Ransomware is commonly spread through phishing attacks or more advanced spear phishing attempts, which rely on social engineering tactics to deceive the victim into opening the file and triggering the attack[3].

---

[1] Gabriel Weimann, *Cyberterrorism: How Real Is the Threat?* Special Report 119, United States Institute of Peace, Washington, DC, 2004, pp. 2-3, https://www.usip.org/sites/default/files/sr119.pdf (02.11.2024)

[2] Li Yuchong, Liu Qinghui, *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments*, "Energy Reports", Vol. 7, 2021, p. 8177, https://www.sciencedirect.com/science/article/pii/S2352484721007289 (02.12.2024)

[3] Maryville University, *Cyber Terrorism: What It Is and How It's Evolved*, https://online.maryville.edu/blog/cyber-terrorism/#examples (26.11.2024)

The development of technological tools in the era of the information society has created new opportunities for cyberterrorist activities, such as identity theft and impersonation, sensitive data breaches for malinformation purposes or shutting down national official information outlets to sow public discord and mistrust in authorities. These new developments of the digital society significantly impact the security of the state. The active use of the Internet and information technologies by various terrorist organizations is one of the new dangerous threats to the global community. In the context of the information society, cyberterrorism has become a significant threat that actively uses the Internet and digital technologies to achieve terrorist goals. Among the main aspects are coordination of actions, information gathering, fundraising, psychological influence, and recruitment of accomplices. The Internet provides terrorist groups with the opportunity to organize operations, reach a broad audience, and even disseminate instructions for creating explosives. As a result, cyberterrorism creates new challenges for state and international security, requiring enhanced coordination to counter this threat.

Conclusions

In the 21st century, cyberterrorism has become a distinct and increasingly prevalent form of terrorism, presenting amplified risks amid widespread digital interconnectivity and limited regulatory oversight. Combating cyberterrorism effectively requires a multi-layered strategy, involving in-depth research, collaboration between governmental bodies and civil organizations, early detection mechanisms, legal framework enhancements, and robust preventive measures. Such a comprehensive approach is essential to minimize vulnerabilities and enhance resilience against cyberterrorist activities on both national and global scales.

The danger of cyberattacks with a terrorist intent or orientation lies not only in the potential for causing significant harm to a large, indeterminate number of individuals but also in the vulnerability of cyberspace to such attacks or terrorist acts and the likelihood of causing enormous material damage. A distinctive feature of terrorist operations is that achieving these objectives does not require substantial investments. From a cost-benefit perspective, cyberspace becomes extremely attractive to terrorists.

Another aspect that deserves attention is the development and evolution of artificial intelligence. We believe that the question of whether the possibilities and opportunities provided by AI will be exploited for malicious purposes is merely a matter of time.

Given the rapid evolution of cyber tactics and geopolitical tensions, future research should also focus on developing proactive countermeasures, analyzing the motivations and tools employed by cyberterrorists, and anticipating potential vulnerabilities within digital infrastructures. As the cyber landscape continues to shift, the alignment of global policy and defense efforts will be crucial in sustaining long-term resilience against cyberterrorism. The ongoing information warfare that underpins current geopolitical conflicts underscores the urgency of these efforts, suggesting that cyberterrorism will likely intensify as a key security challenge in the years ahead.

Bibliography

Books

1. Tropina, Tat'yana, *Kiberprestupnost'. Ponyatie, sostoyanie, ugolovno-pravovye mery bor'by: monografiya*, Vladivostok, 2009
2. Weimann, Gabriel, *Terrorism in Cyberspace: The Next Generation*, New York, 2015

Studies and Articles

1. Barry, Collin, *The Future of Cyber Terrorism*, "Crime & Justice International", Vol. 13, No. 2, March 1997
2. Che, Eliot, *Securing a Network Society: Cyber-Terrorism, International Cooperation, and Transnational Surveillance, Research Paper No. 113*, *Research Institute for European and American Studies (RIEAS*), Athens, September 2007, https://rieas.gr/images/RIEAS113ELIOTCHE.pdf
3. Denning, Dorothy E., *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representative*s, May 23, 2000, https://irp.fas.org/congress/2000_hr/00-05-23denning.htm
4. Denning, Dorothy E., *Is Cyber Terror Next?,* "Social Science Research Council", https://items.ssrc.org/after-september-11/is-cyber-terror-next/
5. Ebner, Nick, *Cyber Space, Cyber Attack and Cyber Weapons A Contribution to the Terminology*, "Institute for Peace Research and Security Policy at the University of Hamburg", Hamburg, October 2015, https://epub.sub.uni-hamburg.de/epub/volltexte/2018/80797/pdf/IFAR2_ FactSheet7.pdf
6. Ejova, Cristina, *Unele abordări conceptuale ale terorismului*, "Studia Universitatis Moldaviae. Științe Sociale", No. 3, 2023, https://social.studiamsu.md/wp-content/uploads/2023/05/31_C_Ejova.pdf
7. Hirschmann, Kai, *The Changing Face of Terrorism*, "International Politics", No. 3, 2000, https://library.fes.de/pdf-files/ipg/ipg-2000-3/arthirschmann.pdf
8. Li, Yuchong; Liu, Qinghui, *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments*, "Energy Reports", Vol. 7, 2021, https://www.sciencedirect.com/science/article/pii/S2352484721007289
9. Mahadevan, Prem, *Cybercrime. Threats during the COVID-19 Pandemic*, Global Initiative Against Transnational Organized Crime, April 2020, https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf
10. Orji, Uchenna, Jerome, *Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States*, "Defense Against Terrorism Review", Vol. 6, No. 1, 2014
11. Pollitt, Mark, M., *Cyberterrorism: Fact or Fancy?*, "Computer Fraud and Security", February 1998
12. Tropina, Tat'yana, *Kiberprestupnost' i kiberterrorizm: pogovorim o ponyatijnom apparate*, in *Informacionnye tekhnologii i bezopasnost. Sbornik nauchnyh trudov mezhdunarodnoj konferencii, Nacional'naya akademiya nauk Ukrainy*, Kyiv, 2003
13. Tuitel, Ruben, *Defining Cyberterrorism*, "PerConcordia: Journal of European Security and Defense Issues", Vol. 7, No. 2, 2016, https://perconcordiam.com/perCon_V7N2_ENG.pdf
14. Weimann, Gabriel, *Cyberterrorism: How Real Is the Threat?*, Special Report 119, United States Institute of Peace, Washington, DC, 2004, https://www.usip.org/sites/default/files/sr119.pdf
15. Wilson, Clay, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues*, October 2003, https://apps.dtic.mil/sti/pdfs/ADA421056.pdf

Documents

1. Center for Strategic and International Studies, *Significant Cyber Incidents,* https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
2. Check Point, *Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks,* July 2024, https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/
3. Digital 2024: Global Overview Report. https://indd.adobe.com/view/8892459e-f0f4-4cfd-bf47-f5da5728a5b5

   4. Maryville University, *Cyber Terrorism: What It Is and How It's Evolved*, https://online.maryville.edu/blog/cyber-terrorism/#examples
5. UN General Assembly, *Resolution A/54/49: Developments in the Field of Information and Telecommunications in the Context of International Security*, December 1, 1999, https://documents.un.org/doc/undoc/gen/n99/777/13/pdf/n9977713.pdf
6. United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes*, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

7. United States Congress, *USA Patriot Act of 2001,* congress.gov/107/plaws/publ56/PLAW-107publ56.htm

Websites

1. https://blog.checkpoint.com/
2. https://www.congress.gov/
3. https://www.csis.org/
4. https://www.unodc.org/
5. https://www.usip.org/