# LEGAL ASPECTS OF DEFINITION OF INTERNATIONAL CYBER TERRORISM

**Nugman A. Nugmanov**

DSc, Professor of the Department of International Law and Public Legal Sciences of UWED

**ABSTRACT**. *The article is devoted to the current problem of international cyberterrorism as one of the dangerous forms of transnational crime. The author analyzes the tendency of terrorist and extremist organizations to use digital technologies to attack government structures, spread extremist propaganda, finance criminal activities, and recruit new participants through Internet resources. The transborder nature of the threat of cyberterrorism is emphasized, that is, the formation of vulnerability in one state can create a risk to comprehensive security at the global level. The article focuses on the fusion of cybercrime with the financing of terrorism and organized crime. The author proposes the development of clear international legal definitions of cyberterrorism and international counteraction mechanisms.*

**KEYWORDS:** *cyberterrorism; transnational crime; international security; information security; terrorist financing; critical infrastructures.*

## INTRODUCTION

Currently, there are increasingly frequent cases of the development of information technologies and computer networks by transnational terrorist and extremist organizations, which has led to the emergence of the most dangerous type of computer crime - computer terrorism or cyberterrorism. According to statements by western intelligence agencies and law enforcement agencies, terrorist organizations are actively using the capabilities of the Internet. Using Internet resources, they carry out information cyber-attacks, propaganda of extremist ideas, racial, religious and other forms of intolerance, as well as recruiting new members, carrying out illegal financial transactions, etc. It should be noted that interstate relations in the field of information exchange are subject to the norms and principles of international law, which regulate various aspects of the dissemination of information at the international level (Nugmanov, 2015).

As has been rightly noted, "the Internet provides terrorists with exceptional opportunities" (Whine, 2008), and "the victims of cyberterrorism will primarily be government organizations and large commercial structures" (Vasiliev, 2000, p. 178). It is obvious that the dangerous trend of merging "cybercrime" and terrorist financing with transnational and organized crime, mainly in the form of illegal production and distribution of narcotic drugs and psychotropic substances, is of particular concern.

It is rightly noted that the interconnectedness of digital infrastructure allows cyber threats to easily cross borders, causing widespread damage. A data breach in one country can impact international markets, highlighting the economic risks of weak cybersecurity (Huang et al., 2021). Attacks on critical infrastructure, like energy grids and healthcare systems, pose national security risks (Lindemulder and Kosinski, 2024).

Undoubtedly, cyberterrorism poses a threat of attack on so-called critical information infrastructures that allow critically important objects (or processes) to function. These include national telecommunications systems, airfields, gas pipelines, etc. As a result of destructive impact on such infrastructures, the probability of a

catastrophic situation caused by disruption of their information systems and fraught with enormous negative consequences on a national scale increases many times over (Nugmanov, 2016).

Although, the term “cyber terrorism” is being used with increasing frequency nowadays, an agreed-upon definition has not been arrived at. The definition of the term “cyber terrorism” has varied from being incredibly broad to being focused. If a too-narrow definition is adopted, it will exclude and lose many of the elements of large-scale cyber-attacks; in contrast, a too-broad definition will include too many of the elements of actual cybercrimes under the category of cyber terrorism (Tehrani et al., 2013).

## SCOPE OF RESEARCH

In the area of research, we highlight several key elements. Firstly, the problem of differentiation of cyberterrorism, namely, a clear distinction between the concept of "cyberterrorism" and related phenomena, such as general computer crime, hacking, cyber warfare and terrorist financing. Secondly, this is the development of a clear and scientifically substantiated definition of the concept of "cyberterrorism", that is, the unification of various types of criminal activity on the network for terrorist purposes, which can be manifested through cyberattacks, propaganda, recruitment, financing. Thirdly, this is the issue of the use of information technology by terrorist organizations, that is, how transnational terrorist and extremist organizations master and use information technology and computer networks (the Internet) for their activities. Fourthly, this is the problem of the transnational nature of the threat and its international legal aspects, since international cyberterrorism is a transboundary threat, which is facilitated by the global nature of the Internet, and obviously affects the issues of its regulation by the norms of international law. Fifthly, this is the consideration of the issues of reducing the risks of terrorist cyberattacks on critical important infrastructures, which can further create risks for the national and economic security of the state. Sixthly, this is the study of the international legal aspects of regulating information exchange and combating cyberterrorism. That is, the Scope of Research of the article focuses on the theoretical and legal aspects of cyberterrorism, primarily on its definition and distinction from related concepts (differentiation), and also covers specific forms of IT use by terrorists, the transnational nature of the threat, risks for critical infrastructure and security and the international legal context of regulation.

## LITERATURE REVIEW

This article aims to fill these gaps, primarily in matters of definition and differentiation. Existing scientific publications and intelligence reports clearly demonstrate the seriousness and growing complexity of the threat of cyberterrorism. However, the key gaps remain the lack of a consensus definition of cyberterrorism and clear criteria for limiting it (differentiating it) from related types of cybercrime and terrorist activity, especially against the background of their dangerous merger with transnational organized crime. Current areas of research include the analysis of the transnational nature of the threat, risk assessment for critical infrastructure and the economy, and the development of adequate international legal mechanisms to counter it.

The term “cyberterrorism” itself appeared in the information technology lexicon presumably in 1997. It was then that FBI Special Agent M. Pollitt defined this type of terrorism as “deliberate, politically motivated attacks on information, computer systems, computer programs and data, expressed in the use of violence against civilian targets by subnational groups or covert agents” (Tropina, 2003).

Should note that the U.S. Federal Bureau of Investigation defines cyberterrorism as any "premeditated, politically motivated attack against information, computer systems, computer programs and data, which results in violence against noncombatant targets by subnational groups or clandestine agents". Per the FBI, a cyberterrorist attack is a type of cybercrime explicitly designed to cause physical harm. Other organizations and experts include less harmful attacks as acts of cyberterrorism, especially when those are intended to be disruptive or to further the attackers' political agenda. The North Atlantic Treaty Organization (NATO), defines cyberterrorism as a cyberattack that uses or exploits computer or communication networks to cause "sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal" (Awati et al., 2024).

Researchers such as M.J. Devost, B.H. Houghton, N.A. Pollard have characterized cyberterrorism, which is a part of information terrorism, as 1) a combination of the criminal use of information systems through fraud or abuse with the physical violence inherent in terrorism; 2) the deliberate misuse of digital information systems, networks, or components of these systems or networks for purposes that facilitate terrorist operations or acts (Devost et al., 1997).

We agree that the difference between cyberterrorism and other cyber-attacks, such as hacking and cracking, is that the cyberterrorists are politically motivated, while other cyber attackers have non-political motives (Iqbal, 2004).

In the opinion of Mehmet F. Bastug and Ismail Onat, in its pure form, cyberterrorism refers to politically or ideologically motivated cyberattacks to coerce or intimidate governments or societies that result in violence, severe economic damage, or significant fear among the public. In a broad sense, it may also incorporate terrorist use of cyberspace, including online information and communication technologies, in furtherance of terrorist objectives (Bastug and Onat, 2024).

Well noted, common crimes are all those that cannot be classified as computer crimes or cybercrimes, or in any other way in particular. Thus, their definition is always determined by process of elimination. For example, theft is a common crime, in the same way that homicide is. If those crimes are committed by means of a drone operated by radio control, they do not classify as cybercrimes. The radio control is a closed system and so it lies outside of the internet. Although both examples can be committed using technology, they escape the phenomenon of computing or execution in cyberspace (Denning, 2000).

It is obvious that cyber terrorism uses the openness of the Internet to discredit governments and states, host terrorist sites, damage and destroy key systems by introducing falsified data or permanently disabling these systems, which generates fear and anxiety, and is a kind of supplement to traditional terrorism (Lux, 2018).

D. Denning reflects: is cyberterrorism the way of the future? For a terrorist, it would have some advantages over physical methods. It could be conducted remotely and anonymously, it would be cheap, and it would not require the handling of explosives or a suicide mission. It would likely garner extensive media coverage, as journalists and the public alike are fascinated by practically any kind of computer attack. One highly acclaimed study of the risks of computer systems began with a paragraph that concludes "Tomorrow's terrorist may be able to do more with a keyboard than with a bomb" (Grinyaev, 2001).

Researcher D. Rakhimov includes socio-psychological and political aspects of this phenomenon in his definition of cyberterrorism, and believes that "Cyberterrorism is a deliberate politically motivated attack on information, computing systems, computer programs or data, carried out by subnational groups or secret agents, the result of which is violence against peaceful targets, creating the danger of loss of life, causing significant property damage or the occurrence of other socially dangerous consequences" (Rakhimov, 2004).

The deliberate nature of this crime is noted by V.A. Golubev, who proposed that cyberterrorism be understood as "a deliberate attack on information processed by a computer, a computer system or network that creates a danger to the life and health of people or the occurrence of other serious consequences, if such actions were committed with the aim of violating public safety, intimidating the population or provoking a military conflict" (Golubev, 2022).

In law, the closest definition is found in the U.S. Patriot Act 18 U.S.C. 2332b's definition of "acts of terrorism transcending national boundaries" and reference to activities and damages defined in the Computer Fraud and Abuse Act (CFA) 18 U.S.C. 1030a-c. Interestingly, the CFA's discussion of the "punishment for an offense" entails fines or imprisonment and suggests that it is a criminal act as opposed to an act of terrorism (U.S. Code, n.d.).

We agree with famous an expert in the field of computer crime research Dorothy Denning's definition of cyberterrorism: "unlawful attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Denning, 2023).

**CORE ISSUE**

The core issue of the article is the problem of defining and distinguishing cyberterrorism, as well as the lack of a clear definition of the concept of "cyberterrorism". Based on the above, it can be stated that there is no single, generally accepted definition of the concept of "cyberterrorism". Terrorist organizations use the Internet for a variety of purposes: information cyberattacks, propaganda of extremism, recruitment, financing, etc. The question arises: which of these acts should be classified as cyberterrorism, and which - as other forms of criminal activity? The task is to develop an accurate and scientifically sound definition of this phenomenon. The next problem is the complexity of differentiating cyberterrorism, namely, there is a serious problem of distinguishing cyberterrorism from related concepts such as general cybercrime (computer crime), cyberwar and terrorist financing. Of particular concern is the dangerous merger (convergence) of "cybercrime" and terrorist financing with transnational organized crime (in particular, with drug trafficking). This merger makes it difficult to clearly identify the terrorist component in

cyberspace. The core issue is the lack of a clear conceptual apparatus: the unresolved question of what exactly should be understood as cyberterrorism (the problem of definition) and how to distinguish it from other, closely intertwined types of illegal activity in cyberspace (the problem of differentiation), especially against the background of their dangerous merger with transnational organized crime. In our opinion, the solution of these problems is a necessary condition for the effective fight against this threat.

In our view, it is clear that the Internet is a clear example of how terrorists can operate across borders, and states need to respond to the challenges of international terrorism on a transnational basis as well. Today, those who want to use cyberspace for terrorist purposes can do so from virtually anywhere in the world. Terrorists are very good at taking advantage of differences in national responses. This means that the global Internet can become a virtual haven for terrorists, which allows them to ignore state borders.

Despite the existence and functioning of a very broad conceptual field of this phenomenon, many normative legal documents both at the national and international levels do not contain a definition of cyberterrorism. For example, the Law of the Republic of Uzbekistan "On Combating Terrorism" of December 15, 2000 - one of the main instruments of criminal-legal regulation of the fight against terrorism in the Republic of Uzbekistan - does not contain a definition of cyberterrorism, and the definition of terrorism does not indicate cyberspace (Law of the Republic of Uzbekistan, 2000). Meanwhile, for example, in the United States after the terrorist attacks on New York and Washington, the US Congress adopted a new US anti-terrorism law - "The Act to unite and strengthen America by providing adequate means to intercept information and prevent terrorism (US Patriot Act of 2001)" (U.S. Patriot Act, 2001). By this law, Congress created a new statutory concept of "cyberterrorism" and included in it various qualified forms of hacking and damage to the protected computer networks of individuals, legal entities, and government agencies, including damage caused to a computer system used by a government agency in organizing national defense or ensuring national security.

Similar processes are underway in European countries. The issue of legal and organizational mechanisms for regulating the use of computer networks is being promoted to the category of priorities. The first international agreement on legal and procedural aspects of the investigation and prosecution of cybercrimes was the Convention on Cybercrime, adopted by the Council of Europe on November 23, 2001 (Convention on Cybercrime, 2001). The Convention provides for coordinated actions at the national and interstate levels aimed at preventing unauthorized interference in the operation of computer systems.

The particular danger of computer crime and cyber terrorism, both from the point of view of national and international law, is obvious. Being a special dimension of terrorist activity with a specific causal basis, they determine the need to adopt comprehensive, special measures that exercise control over it and contribute to the effective fight against this destructive criminal activity.

The fight against cybercrime is complicated by the fact that today it is practically impossible to predict or track a computer attack in real time, since it can be carried out by a variety of people located

anywhere on the planet. Reliably identifying the people behind the attack will require a lot of time and considerable resources. This also actualizes the problem of international cooperation in law enforcement procedures regarding the search, capture or extradition of criminals using the global Internet and modern types of ICT. It should be noted that today international cooperation in interaction in the fight against terrorism, including cyberterrorism, is not at the proper level.

It is also important to consider the fact that any, even the most effective fight against illegal, criminal acts is inferior in achieving results to their prevention. Unfortunately, the intensification of terrorist propaganda is carried out mainly through cyberspace. Any type of terrorism, including cyberterrorism, is one of the threats generated by objective reality in the modern conditions of an interconnected and interdependent, globalizing world, which actualizes the problem of counteracting it. According to the general definition of the "Dictionary of Basic Terms and Concepts in the Sphere of Combating International Terrorism and Other Manifestations of Extremism" prepared by the Anti-Terrorism Center of the CIS Member States, terrorist propaganda is the dissemination in written, oral and visual-demonstration form of ideas, views, theories justifying terrorism and the need to carry out terrorist activities, as well as calls for their implementation; as well as the production and storage of relevant materials for these purposes (CIS Anti-Terrorism Center, n.d.). In this sense, to neutralize the threats of terrorism, it is necessary to unite and cooperate with states at the international level not only to destroy, but also to prevent the social, ideological and economic causes of terrorism.

A comprehensive approach is needed to combat cybercrime and cyberterrorism, as well as their prevention. It is obvious that the dynamics of development of international legal norms should correspond to the development of information technologies, which are developing extremely dynamically. Therefore, there is a need to unify national legislation and expand the international legal framework, ensuring the implementation of an effective system for preventing and stopping possible criminal use of ICT.

The solution of these tasks largely depends on the organization of coordination of the activities and interaction of special services, law enforcement agencies, the judicial system in the field of information security and, accordingly, providing them with the necessary modern material and technical base. It is also important to consolidate at the legislative level the provision on ensuring the information security of state and private complexes of information systems, resources and databases and the provision on the rights of law enforcement agencies to monitor virtual space, and the implementation on their part of measures to stop the activities of Internet resources of a terrorist nature, as well as those promoting war, racial and religious intolerance, pornography, pedophilia, etc.

We agree that as cyber threats escalate, cohesive international legal frameworks for cybersecurity and data protection are urgently needed. Countries are recognizing the ineffectiveness of a fragmented approach, prompting efforts to establish international standards and cooperative policies to strengthen global responses to cybercrime (World Economic Forum, 2024).

In our opinion, when creating and using open international information networks and when organizing information exchange at the international level, it is necessary to develop interstate cooperation in the formation of international standards for the implementation of a unified approach to ensuring information security of both information resources and information and communication systems. In this regard, one of the priority trends in the fight against modern high-tech types of crime, including cyberterrorism, is the development of a unified conceptual apparatus and the development of coordinated measures in the field of combating cybercrime.

It is necessary to note here that in the modern period there is a merging of the activities of individual hacker groups and the activities of security agencies of a number of states, when hacker groups arise or are hired for the activities of individual states. In such a case, "cyberterrorism" becomes the lot of not only individuals or groups, but also of states.

According to their target settings, computer offenses falling under the category of cyberterrorism can be divided into two types. The first of these includes terrorist acts committed through the use of computers and cyberspace, and the second includes acts when information and communication networks are used for terrorist purposes, but not for the direct commission of terrorist acts.

In accordance with the first type, the definition of cyberterrorism arises by combining the concepts of "terrorism" and "cyberspace". Terrorism, in accordance with Art. 155 of the Criminal Code of the Republic of Uzbekistan (Law of the Republic of Uzbekistan, 2000), is violence, use of force, other acts that create a danger to a person or property, or a threat to commit them in order to compel a state body, international organization, their officials, an individual or legal entity to commit or refrain from committing any activity in order to complicate international relations, violate sovereignty and territorial integrity, undermine state security, provoke war, armed conflict, destabilize the socio-political situation, intimidate the population. It follows that cyberterrorism is a deliberate attack on computers, information and communication networks or computer programs, or the use of a telecommunications network and the global information network Internet in order to create a danger to the life of an individual or cause property damage, or the occurrence of other socially dangerous consequences. This act must be carried out with the aim of complicating international relations, violating sovereignty and territorial integrity, undermining state security, provoking war or armed conflict, disrupting the socio-political situation, intimidating the population in order to influence decision-making by the authorities of an international organization, their officials, an individual or legal entity. This type of terrorism may also include the threat of carrying out such actions to achieve the above goals.

Another type of cyberterrorism, i.e., as they say, "not in its pure form", can include the actions of terrorist groups that use global information networks not to directly commit terrorist acts, but to popularize the activities of the organization or other similar actions. Such actions in cyberspace can include: obtaining information on suspected terrorist targets, etc.; searching for sponsors of terrorist movements; creating websites for subsequent posting of various information on the activities of terrorists; giving large-scale publicity to responsibility for committing a terrorist act; disseminating various alarming rumors to

sow panic, etc.; using encrypted e-mail; disseminating information of a terrorist nature (instructions for making explosive devices on your own, etc.). Of course, this is not a complete list of the ways in which terrorist groups can use the global Internet for their own purposes.

Not by chance in the United Nations Global Counter-Terrorism Strategy Resolution adopted by the General Assembly of the United Nations at 30 June 2021 noted that "terrorists may craft distorted narratives that are based on the misinterpretation and misrepresentation of religion to justify violence, which are utilized to recruit supporters and foreign terrorist fighters, mobilize resources and garner support from sympathizers, in particular by exploiting information and communications technologies, including through the Internet and social media, and also notes in this regard the urgent need for the international community to globally counter such activities" (UN Global Counter-Terrorism Strategy, 2021).

Thus, the problems of differentiation and definition of cybercrime, namely cyberterrorism, the fight against this illegal, destructive phenomenon, the problems of prevention and ensuring the security of cyberspace, identified in the course of a thorough study of this phenomenon, as well as a deep analysis of legislation in the field of information and its protection both at the national and international levels, necessitate the need to fill the existing gaps in the field of legal regulation.

We agree with the opinion that the intensification of lawmaking in the information sphere in the last few years inevitably leads to an increase in the number of legal acts, which often contain contradictory legal norms. Many researchers, noting various aspects of the imperfection of information legislation, are convinced of the advisability of its systematization in order to eliminate these contradictions by codifying legislation in this area, which should go in parallel with the process of rulemaking (Veprentseva, 2022).

It is rightly noted that in order to reduce the risk of cyberterrorist attacks, the same means can be used that are used to maintain and protect communications during natural disasters. This factor is a smart investment that will serve to protect against cyberterrorism, since businesses and government agencies are not fully prepared for cyber threats and cannot always repel them (Tambiev and Kochesokova, 2023). In addition, an important problem in the fight against cyber terrorism is that law enforcement agencies have a shortage of technical equipment in the form of special software. Because of this, time is lost, it is not possible to document the crime in a timely and complete manner and identify the persons involved in its commission (Lobach, 2022).

Well noted, that in the past, cyberterrorism mostly targeted government entities. But now, businesses and other organizations are becoming targets as well, so they must implement extensive cybersecurity measures and vigilance to counter cyberterrorism. For one, they must ensure that all internet of things devices is secured and inaccessible via public networks. To protect against ransomware and similar types of attacks, they must backup systems regularly and implement continuous monitoring techniques. They must also use firewalls, antivirus software, and antimalware to protect their systems from these attack vectors. Companies must also implement controls and IT security policies to protect business data. This includes limiting

access to sensitive data and enforcing strict password and authentication procedures, like two-factor authentication or multifactor authentication (Awati et al., 2024).

## EXECUTIVE SUMMARY

It is obvious that the key problem in the differentiation and definition of the concept of cyberterrorism is the lack of a clear definition and reliable criteria for distinguishing (differentiating) the concept of "cyberterrorism" from related phenomena, such as cybercrime and terrorist financing (Tehrani et al., 2013). Particular relevance of this problem is given by the dangerous trend of merging (convergence) of cybercrime and terrorist financing with transnational organized crime (Huang et al., 2021). Today, transnational terrorist and extremist organizations are actively mastering information and communication technologies and the Internet. They use them for information cyberattacks, propaganda of extremism, recruitment of new members and implementation of illegal financial transactions (Nugmanov, 2015). And naturally, the global Internet provides terrorists with exceptional opportunities for cross-border activities (Whine, 2008).

Cyberterrorism poses a global threat to both government organizations and large commercial organizations, and can pose enormous risks to critical infrastructures, i.e. energy systems, healthcare systems, etc. and thus pose threats to national security (Lindemulder and Kosinski, 2024). In addition, it is obvious that data security breaches and cyber attacks in one country can cause a cascading effect and significant losses in international markets, thereby causing enormous economic damage at the international level (Huang et al., 2021). An important aspect is that, due to the interconnectedness of digital infrastructure, the threat of cyber terrorism easily crosses borders and can cause large-scale damage (Bastug and Onat, 2024). And an absolutely important aspect is that the fight against this transnational threat requires the regulation of interstate relations in the field of information exchange by the norms and principles of international law (Nugmanov, 2015). Analysis and solution of the problems of definition and differentiation of cyber terrorism is a necessary basis for understanding this threat and developing effective countermeasures, especially in the context of its merger with other forms of transnational crime.

Based on the above and relying on the need to counter the propaganda of terrorism, cyberattacks and other types of cybercrime carried out mainly in cyberspace using ICT, we consider it expedient: firstly, to develop a concept of counter-propaganda of terrorism, including cyberterrorism among the population, especially among young people, with a thorough, detailed description of the main principles and specific areas of countering the propaganda of these antisocial phenomena; secondly, to improve the monitoring of websites, media space, the system of information (media) education; regularly update popular Internet resources with interesting analytical information of an educational nature. In order to strengthen the ideological component of the education of the younger generation, create children's, adolescent, youth websites, information platforms with interesting offers (for example, educational games, entertainment programs, media competitions, etc.) that meet the spiritual and moral needs of modern youth; thirdly, to strengthen the research work of relevant scientific institutions and educational institutions on the problems of ICT, cyber education, counteraction to cyber terrorism,

etc. Regularly publish cycles of scientific-methodological and educational-methodological manuals for young people with open developments based on real examples of cyber propaganda, recruitment with their detailed analysis, conclusions and specific recommendations of a counter-propaganda nature; fourthly, to improve the system of professional training of specialists in cyber education, cyber security, media education, as well as psychological rehabilitation of those who ended up in the cybercriminal space due to their computer addiction or other socio-psychological reasons; fifthly, to improve the activities of public organizations, civil institutes, schools and other educational institutions aimed at cyber education, educating young people in the spirit of patriotism, tolerance, counteraction to propaganda of all manifestations of terrorism, including cyber terrorism (UN Global Counter-Terrorism Strategy, 2021).

## REFERENCES


1. Awati, R., Sheldon, R. and Hanna, K.T., 2024. Definition cyberterrorism. *TechTarget*. Available at: https://www.techtarget.com/searchsecurity/definition/cyberterrorism [Accessed 9 February 2024].

2. Bastug, M. and Onat, I., 2024. Cyberterrorism. *Oxford Research Encyclopedia of Criminology*. Available at: https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-790 [Accessed 20 March 2024].

3. CIS Anti-Terrorism Center, n.d. Dictionary of Basic Terms and Concepts in the Sphere of Combating International Terrorism and Other Manifestations of Extremism. Available at: https://www.cisatc.org/1289/136/149/159 [Accessed 31 July 2025].

4. Convention on Cybercrime, 2001. Budapest, 23 November 2001. Council of Europe. Available at: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/rms/0900001680081580 [Accessed 31 July 2025].

5. Denning, D.E., 2000. Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, 23 May 2000. *Terrorism Research Center*.

6. Denning, D.E., 2023. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Available at: http://www.crime.vl.ru/docs/stats/stat_92.htm [Accessed 31 July 2025].

7. Devost, M.G., Houghton, B.K. and Pollard, N.A., 1997. Information terrorism: Political violence in the information age. *Terrorism and Political Violence*, 9(1), pp.72-83.

8. Golubev, V.A., 2022. Cyberterrorism - a threat to national security. Available at: http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism [Accessed 31 July 2025].

9. Grinyaev, S.N., 2001. Information terrorism: prerequisites and possible consequences. *Journal of the Theory and Practice of Eurasianism*, (19), pp.31-35.

10. Huang, K., Madnick, S. and Zhang, F., 2021. Navigating cybersecurity risks in international trade. *Harvard Business Review*. Available at: https://hbr.org/2021/12/navigating-cybersecurity-risks-in-international-trade [Accessed 2 December 2021].

11. Iqbal, M., 2004. Defining cyberterrorism. *John Marshall Journal of Computer & Information Law*, 22(2), pp.397-408.

12. Law of the Republic of Uzbekistan, 2000. On Combating Terrorism, 15 December 2000. Available at: https://lex.uz/docs/111457 [Accessed 31 July 2025].

13. Lindemulder, G. and Kosinski, M., 2024. What is cybersecurity? *IBM*. Available at: https://www.ibm.com/topics/cybersecurity [Accessed 12 August 2024].

14. Lux, L.M., 2018. Defining cyberterrorism. *Revista Chilena de Derecho y Tecnología*, 7(2), pp.31-45. Available at: http://dx.doi.org/10.5354/0719-2584.2018.51028 [Accessed 31 July 2025].

15. Nugmanov, N.A., 2015. International law regulation of cooperation in the sphere of international information exchange. *Bulletin of the Volga Region Institute of Administration*, (2), p.40. Available at: http://vestnik.pags.ru/vestnik/archive/vestnik-47.php [Accessed 31 July 2025].

16. Nugmanov, N.A., 2016. Problems of formation of international standards for implementation of a unified approach to ensuring information security. *International Relations*, (2), pp.64-70.

17. Rakhimov, D.F., 2004. Modern constructions of the definition of terrorism: international legal aspects. Tashkent: Qonun Himoyasida, p.82.

18. Tambiev, S.A. and Kochesokova, Z.Kh., 2023. International experience in countering cyberterrorism. *Law and Management*, (2), pp.161-165.

19. Tehrani, P.M., Manap, N.A. and Taji, H., 2013. Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law & Security Review*, 29(3), pp.207-215.

20. Tropina, T.L., 2003. Cybercrime and cyberterrorism: let's agree on the concepts. In: *Problems of crime: traditional and non-traditional approaches*. Moscow: Russian Crime Association, pp.14-21.

21. UN Global Counter-Terrorism Strategy, 2021. Resolution adopted by the General Assembly of the United Nations, 30 June 2021. Available at: https://docs.un.org/en/A/RES/75/291 [Accessed 31 July 2025].

22. U.S. Code, n.d. 18 U.S.C. § 2332b - Acts of terrorism transcending national boundaries. Available at: https://www.law.cornell.edu/uscode/text/18/2332b [Accessed 31 July 2025].

23. U.S. Patriot Act, 2001. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. Available at: https://www.govinfo.gov/app/details/PLAW-107publ56/related [Accessed 31 July 2025].

24. Vasiliev, V.L., 2000. Psychology of terrorism. In: *Modern Terrorism: Status and Prospects*. Moscow: Editorial, p.178.

25. Veprentseva, T.A., 2022. Actual problems of legal support of information security. *National Security / Nota Bene*, (2), pp.59-73.

26. Whine, M., 2008. Cyberspace: A new medium for communication, command and control by extremists. *International Institute for Counter-Terrorism*. Available at: http://www.ict.org.il/ [Accessed 31 July 2025].

27. World Economic Forum, 2024. Cybersecurity rules saw big changes in 2024: Here's what to know. Available at: https://www.weforum.org/stories/2024/10/cybersecurity-regulation-changes-nis2-eu-2024/ [Accessed 17 October 2024].