Received: 11.04.2026. Accepted: 21.04.2026. Available online: 23.04.2026.

МРНТИ 10.87.51
DOI: https://www.doi.org/10.32523/2791-0954-2026-17-1-43-51

Cyberterrorism as a modern security threat: challenges and counter-measures

Nizamov Muhammadamin
Master student, Academy of public administration under the President of Republic of Tajikistan
Dushanbe, Tajikistan
e-mail: nizomov.m04@gmail.com

Abstract: This paper examines cyberterrorism as a challenge to international security. Its features, hybrid forms, and counteraction mechanisms within the SCO, the UN, and Interpol are analyzed. The methodological basis of the study is based on comparative legal and institutional analysis, as well as analysis of specific precedents, which allows us to trace the evolution of the threat and the response of the international community. Special attention is paid to the role of artificial intelligence and the need to maintain a balance between security and human rights. The study concludes that cyberterrorism has gone beyond the traditional understanding of terrorism in cyberspace. To increase efficiency, it is proposed to develop the integration of countries' security systems, create joint training centers and share experiences in the fight against cybercrime.

Keywords: cyberterrorism, international security, financing of terrorism, SCO, UN, Interpol, artificial intelligence, human rights, international cooperation.

Кибертерроризм қазіргі қауіпсіздікке қауіп тондіреді: қиындықтар мен қарсы шаралар

Низамов Мухаммадамин
Магистр, Тәжікстан Республикасы Президентінің жанындағы Мемлекеттік басқару Академиясы
Душанбе, Тәжікстан
e-mail: nizomov.m04@gmail.com

Аннотация: Бұл мақалада кибертерроризм халықаралық қауіпсіздікке қауіп төндіретін мәселе ретінде қарастырылады. Оның белгілері талданады, гибридті формалары, ШЫҰ, БҰҰ және Интерпол шеңберіндегі қарсы іс-қимыл тетіктері талданады. Зерттеудің әдіснамалық негізі салыстырмалы құқықтық және институционалдық талдауға, сондай-ақ қауіптің эволюциясы мен халықаралық қауымдастықтың реакциясын бақылауға мүмкіндік беретін нақты прецеденттерді талдауға негізделген. Жасанды интеллекттің рөліне және

қауіпсіздік пен адам құқықтары арасындағы тепе-теңдікті сақтау қажеттілігіне ерекше назар аударылады. Зерттеу кибертерроризм киберкеңістіктегі терроризм туралы дәстүрлі түсініктен асып түсті деген қорытындыға келді. Тиімділікті арттыру үшін елдердің қауіпсіздік жүйелерінің интеграциясын дамыту, бірлескен оқу орталықтарын құру және киберқылмыспен күресте тәжірибе алмасу ұсынылады.

Түйінді сөздер: кибертерроризм, халықаралық қауіпсіздік, терроризмді қаржыландыру, ШЫҰ, БҰҰ, Интерпол, жасанды интеллект, адам құқықтары, халықаралық ынтымақтастық.

Кибертерроризм как современная угроза безопасности: вызовы и меры противодетсвия

Низамов Мухаммадамин
Маистр, Академия государственного управления при президенте Республики Таджикистан
Душанбе, Таджикистан
e-mail: nizomov.m04@gmail.com

Аннотация: В данной работе исследуется кибертерроризм как вызов международной безопасности. Анализируется его признаки, гибридные формы, а также механизмы противодействия в рамках ШОС, ООН и Интерпола. Методологическая база исследования основано на сравнительно-правовом и институциональном анализе, а также анализе конкретных прецедентов, что позволяет проследить эволюцию угрозы и ответные меры международного сообщества. Отдельное внимание уделяется роли искусственного интеллекта и необходимости соблюдения баланса между безопасностью и правами человека. В результате исследования приводится вывод о том, что кибертерроризм вышел за рамки традиционного понимания терроризма в киберпространстве. Для повышения эффективности предлагается развивать сопряжение систем безопасности стран, создание совместных учебных центров и делится опытам в борьбе с киберпреступлениями.

Ключевые слова: кибертерроризм, международная безопасность, финансирование терроризма, ШОС, ООН, Интерпол, искусственный интеллект, права человека, международное сотрудничество.

Introduction

The evolution of information and communication technologies has changed the face of international relations. Along with the development of technology, the digital age has created new challenges. Cyberspace, which knows no state borders, has turned into an arena of confrontation, where terrorist groups have access to tools capable of causing damage that are comparable to the consequences of classic terrorist attacks.

Today, cyberterrorism is no longer limited to attacking computer networks, it also includes the possibility of using cryptocurrencies to finance terrorist organizations.

It is alarming that not only civilian infrastructure, but also defense enterprises are increasingly becoming targets of cyber attacks. The defeat of these facilities, in turn, will lead to the paralysis of entire regions, and as a result of these attacks, the possibility of international conflicts is not excluded. In these circumstances, the development of an effective mechanism to counter cyberterrorism is becoming an issue of international security.

In addition to the technical impact on infrastructure, cyberterrorism also performs a psychological function, which was previously typical of classical terrorism (an atmosphere of fear and insecurity). Widespread coverage of hacking of government portals, leakage of personal data and the threat of disabling the life support system create a sense of vulnerability of the state among the population. In this regard, we can say that programs of digital "hygiene" of the population are needed.

In these circumstances, the development of an effective mechanism to counter cyberterrorism is becoming an issue of international security. International and regional organizations are rapidly trying to combine the efforts of law enforcement agencies to establish rapid data exchange to counter cyber attacks.

However, the rapid development of artificial intelligence creates both new opportunities to combat cyber threats and raises complex issues related to maintaining a balance between ensuring security and protecting fundamental human rights and freedoms.

Object of research: Cyberterrorism as a complex problem of international law, posing a threat to international and national security.

The subject of the study: Complex characteristics, forms of occurrence, methods of financing cyberterrorism by transferring cryptocurrencies, attempts to counter international and regional organizations, the role of artificial intelligence in identifying cyberterrorist threats.

The aim of the study is to analyze cyberterrorism as a modern challenge to international law, identify key features, develop forms and methods, and develop recommendations for improving international cooperation to counter this phenomenon while respecting basic human rights and freedoms.

Research objectives:

1. Analysis of existing approaches to identify cyberterrorism

2.Identification of factors contributing to the spread of cyberterrorism

3. Identification and systematization of the main forms of cyberterrorism, including classical cyber attacks and hybrid forms

4. Assessment of the effectiveness of existing international mechanisms for countering cyberterrorism within the SCO, the United Nations and Interpol.

5. Investigation of the potential and risk of using artificial intelligence in the fight against cyberterrorism.

Methods and approaches: The study uses comparative legal analysis, the method of institutional analysis, as well as the analysis of specific examples.

Hypothesis: As a result of the evolution of cyberterrorism, it has gone beyond the traditional understanding of terrorism in cyberspace. The hybridization of its form and the vulnerability of civilian and military infrastructure require not only the strengthening of the system, but also the development of a unified system of international and legal mechanisms. At the same time, efficiency cannot be maintained without maintaining a balance between security measures and the protection of fundamental rights and freedoms of citizens.

Research methods

This study is aimed at identifying and studying the definitions of cyberterrorism, international conventions, the UN resolution and the SCO declaration were also considered. The use cases were considered as an illustration of threats and vulnerabilities.

Discussion

The word “cyberterrorism” has long been part of the scientific community. But still, there are different position from different countries and experts on what exactly is meant by sweat by this word.

There is an opinion that cyberterrorism is “the commission of terrorist acts in cyberspace” or, as some experts write, that “it is advisable to consider cyberterrorism as a complex of illegal actions in the information space, representing attacks on computer and telecommunications technologies aimed at creating a threat to international and state security in order to influence political, economic and other decisions”.

There is also an opinion among Western experts that “cyberterrorism generally refers to extremely destructive computer attacks or threats of attacks by non-state actors on information systems carried out with the aim of intimidating or forcing governments or society to achieve goals of a political or social nature”.

We can agree with each of these authors, but it is important to mention that cyberterrorism is not only the commission of terrorist acts on computer network, which is a classic form, but also its hybrid form, when digital money is used for the benefit of certain prohibited organizations or groups, which is regarded as terrorist financing.

It’s worth asking the question, where do they come from (hackers, some of whom become cyberterrorism)? We think the answer is very obvious, there are funded by certain individuals (it is also assumed that they are funded by states to achieve their political goals) through money transfers. In this regard, it should be emphasized that as technology develops in the field of economics, as well as the emergence of new exchanges and financial markets, it leads to the fact that if someone has transferred a certain amount of money to a terrorist organization, tracking this transaction becomes difficult or even impossible. For example, by sending money in the form of cryptocurrencies using cold wallets.

Cryptocurrency exchanges and exchangers are often registered in offshore zones or states with no strict AML/CFT regulations (these are two international standards and measures to prevent money laundering or blocking cards with questionable

transactions), which allows attackers to send or receive money in the form of cryptocurrencies without any special obstacles.

With the development of technology and the widespread availability of information and communication technologies, extremist and terrorist organizations have gained the opportunity to actively use internet resources and social media for a range of illegal activities. This includes incitement to violence, radicalization, finding new supporters, conducting training, detailing plans, gathering intelligence information, establishing contacts, conducting propaganda and raising funds.

It is worth mentioning that the globalization of the modern economy, as well as every sphere of life of ordinary citizens, such as communications, energy, financial and banking systems, gas and oil storage systems, the state defense system, etc. are the biggest reason for the increasing spread of cyberterrorism.

Despite all the above-mentioned destructive factors, it is also worth emphasizing that the latest technologies enable law enforcement agencies to effectively counter terrorism and cyberterrorism with the necessary observance of international law.

Another difficulty is the identification of the attacker. Unlike the classic type of terrorism, when the perpetrator is directly at the scene of the crime, in cyberterrorism it is often very difficult to legally prove whether the state, a terrorist organization or individual funded individuals were behind this attack.

Some experts note that “international communities are coming together to solve the problems of combating cybercrime. Evidence of this is the meeting of the Shanghai Cooperation Organization [SCO] member countries in Astana in April 2012, where a Protocol on cooperation was signed, which defined the main areas of cooperation between the Ministry of Internal Affairs of Russia and the ministries of public security of the SCO countries in the near future, as well as measures to combat crime in the field of information technology and illegal internet usage”. The Astana Declaration of the Council of Heads of SCO Member States of July 4, 2024 calls on the SCO member states to develop a document on cooperation in combating crimes in the field of information technology.

Interpol’s activities are guided primarily by the Budapest Convention on Cybercrime {No. 185, 2001}. Despite the fact that both organizations have independent strategies, they share a common goal – to increase cybersecurity. Interpol focuses on developing innovative investigative techniques and rapid data exchange.

Cooperation is actively developing in the field of professional development of law enforcement officers. Since 2023, a joint training center has been operating in Tashkent, which conducts certified training on investigating cryptocurrency fraud and countering cyber attacks. Combining Interpol’s methodologies and the specifics of the Eurasian region.

The key achievement of the two organizations is the interfacing of systems. The SCO platform, which monitors cyber attacks on important facilities, is integrated with the Interpol l-24/7 global secure network. This system makes it possible to instantly transmit data on transnational incidents, in short, when an attempted cyberattack is

recorded in one SCO country, Interpol can immediately alert the rest of the member countries.

CT TECH – A United Nations initiative to create a legislative framework, transparency mechanisms, and oversight regarding online data collection. At the heart of all the work carried out under this initiative is the idea that countries cannot fight technological terrorism alone or using old methods. The UN recognizes that the capabilities of countries vary greatly. The national assessment of risks and equivalent impact measures makes it possible to assess where exactly there are gaps: in legislation, in operational readiness, in investigative techniques or in political planning.

The UN focuses on legal enforcement and calls on countries not only to catch terrorists, but to do so in such a way that the collected digital evidence is indisputable in court and obtained within the framework of the law. In this context, the UN also emphasizes the need to maintain a legal and ethical balance; "The international community is often late in responding". But at the same time, it warns that panic and a desire to "tighten the screws" can lead to another problem: unjustified restrictions on human rights, in particular, the right to privacy and freedom of expression.

In the context of terrorism, intelligence agencies want to collect data, and the more the better. However, the UN insists that total or uncontrolled surveillance undermines trust in the state and sets a precedent for abuse. The principle of "human rights by default" means that any counter-terrorism action in cyberspace must be designed in advance to protect civil liberties as much as possible.

The fight against cyberterrorism by its very nature cannot be a purely national task, since the Internet has no borders. Therefore, the UN appeals are global and systemic in nature.

The terrorists do not build their own server farms, they use existing and publicly available platforms like X (Twitter), YouTube, and various messengers. UN Security Council Resolution 2396 is a direct call to states that they must not only fight terrorists, but also establish cooperation with the private sector. Information and communication technology companies are becoming key players in this fight, as they have the data and the ability to quickly delete content.

Terrorist organizations are actively developing and even hybridizing their activities, using digital money, social platforms, and new technologies to recruit, finance, and plan attacks.

The UN's work is aimed at providing States not just with recommendations, but with specific tools. This initiative is a call for legal modernization and operational capacity building. At the same time, the international community, as the UN itself has rightly pointed out, is in a precarious position. Panic and the desire for total security must not be allowed to lead to unjustified restrictions on basic human rights, first of all, the right to privacy and freedom of expression.

Success in the fight against cyberterrorism will depend not only on technical equipment, but also on the ability of the global community to ensure a delicate balance between innovation and security. Otherwise, overreaction can lead to great damage to democratic values.

Due to the growing trend in the development of Artificial Intelligence (hereinafter AI), a weighty question arises, "what is the role of AI in the fight against cyberterrorism?" The usefulness of AI in the fight against cyberterrorism is primarily the analysis of large amounts of data. For example, in 2016, China created one of the most powerful computers that can use AI to analyze hundreds of thousands of surveillance camera recordings in a short time, which a person is physically unable to do. In this context, we can say that AI can warn those involved in security in advance or even prevent it (most likely, this can be expected in the near future) an attempted cyberattack on certain military or civilian infrastructure.

There is also a big trend towards introducing AI into every area of human life. Some may think that this somehow infringes on their rights (this is another matter for discussion), but you also need to think about the positive aspects of this. AI can not always be used for selfish purposes, such as disinformation or the creation of fake videos and photos, but also to expose or identify this fake. In this context, AI helps not only to identify potentially cyberterrorist acts, but also physical terrorism. For example, if marketplaces implement AI (which some of them have done), a person's purchase history will be saved in the database and analyzed, as a result, you can summarize what the person is going to do.

Yes, one can agree with the thesis that this infringes on basic human rights and freedoms, but in the context of the fight against terrorism and cyberterrorism, it is a very useful tool for the state. In support of this thesis, we can cite the example of Stuxnet. Stuxnet is a computer worm that became famous after the attack on Iran's nuclear power plant in 2010. Some experts call it the world's first cyber weapon capable of damaging nuclear centrifuges, which could lead to catastrophic consequences. Unlike viruses, worms do not require user activation, they themselves penetrate the computer system and overload it.

The nuclear facility was isolated from the Internet, and the worm was introduced by connecting a USB drive to the main computer. The worm changed the rotation speed of the centrifuges, speeding it up and slowing it down. As a result, about 1,000 centrifuges were disabled. Fortunately, the worm was found and eliminated, it is difficult to imagine what would have happened if, as a result, the attackers' plans had come true.

Or we can give an example of the case of New Petya or Not Petya that occurred in 2017. The virus infected computers that used Windows, also encrypted files, and demanded payment in bitcoins as a ransom. There were attempts to decrypt the files, but instead of opening access to the files, they were deleted.

Ukraine was the first country to be affected, and it lost about 10% of its files, but other countries such as the United States, Australia, Russia, Canada, and government agencies in some European countries suffered enormous damage. Among the companies that were affected were Rosneft, Bashneft, Merck, Maersk and Barispol Airport. The total amount of damage amounted to more than 10 billion dollars.

There have also been cases of dating sites being hacked, for example, Ashley Madison, from where the data of about 40 million users was leaked. Some of them

received threatening messages and ransom demands. It is reported that some of these users, fearing shame, committed suicide.

Just here, an artificial intelligence system would be needed that could calculate in advance the presence of such viruses or worms in the operational system. The above examples also prove that the presence of AI, though not directly, but even indirectly could save the lives of some people.

To be fair, it must be said that AI can also be used by terrorists for various purposes, from hacking the banking system to the country's air defense system, which is the negative side of AI. But to win this fight, you need to be one step ahead. As cyberspace develops, countries need to develop even more and find ways to solve this problem.

Conclusion

It should be noted that such a modern phenomenon as cyberterrorism is one of the most complex and rapidly developing challenges to international security. As a result of the analysis, it was found out that this phenomenon can not only be understood as terrorism in cyberspace, but it can also include several other aspects from financing banned organizations using cryptocurrencies to the active use of social networks to recruit and coordinate illegal actions.

It was also found out that cyberterrorism is a multidimensional threat that should be studied even more deeply and the countries of the world community should solve this problem. Of course, as already mentioned, States are solving these problems within the framework of the Shanghai Cooperation Organization, Interpol and the United Nations, but as we see it, these efforts are not enough to combat this phenomenon more effectively.

If we talk about proposals and ways to solve this problem, then the governments of the countries should work even more and even more closely to create joint training centers, it is also worth combining the data exchange system and developing a unified approach to the investigation of cybercrimes.

It is necessary not to separate from this topic what we said earlier – Artificial Intelligence. This is one of the most useful tools of our time in the fight against cyberterrorism, which is only worth its data processing ability, which will also be useful to integrate and start using in the security system. In this regard, we should also note that the use of AI should not be aimed at violating the freedom of ordinary citizens. It should be aimed solely at the benefit of society.

References

1. Malik, E. N. Cyberterrorism as a global threat: challenges and measures to combat. Bulletin of the Kama Social University. 2020. p. 170

2. Dorothy, E. A View of Cyberterrorism Five Years Later. Center on Terrorism and Irregular Warfare Naval Postgraduate School. p. 2

3. Ovchinnikov, O.A. Scientific support of law enforcement activities of the internal affairs bodies of the Russian Federation: problems and prospects. Administrative law and Process. 2012. N 4. P. 34.

4. Sergevnin, S. L., Alekseev, G. V., Kalkei, E. I. /Interaction of the Shanghai Cooperation Organization with Interpol in the context of combating cybercrime. RANEPA. 2025.

5. Astana Declaration of the Council of Heads of SCO Member States. Shanghai Cooperation Organization. https://rus.sectsco.org/20240704/1420683.html (accessed 20.03.2026)

6. United Nations Counter-Terrorism Office (CTO), 2024/ https://www.un.org/counterterrorism/sites/default/files/law_enforcement_capabilities_framework_for_new_technologies_in_countering_terrorism_finalout_web_ru.pdf (accessed 21.03.2026)

7. United Nations Counter-Terrorism Office (CTO), 2024/ https://www.un.org/counterterrorism/sites/default/files/law_enforcement_capabilities_framework_for_new_technologies_in_countering_terrorism_finalout_web_ru.pdf (accessed 21.03.2026)

8. S/RES/2396(2017) https://main.un.org/securitycouncil/ru/content/sres23962017 (accessed 21.03.2026)

9. https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/ (accessed 22.03.2026)

10. https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked (accessed 22.03.2026)