British Journal of Global Ecology and Sustainable Development
Volume-32, September- 2024
ISSN (E): 2754-9291

THE PROBLEM OF THE XXI CENTURY-CYBERTERRORISM AND COMBATING IT

Maxamadov Rustam Xabibullaevich,
Teacher of the Department of Digital Technology and Information
Security of the Academy of the Ministry of Internal Affairs, Independent Researcher

Djamatov Mustafa Xatamovich,
Senior Lecturer of the Department of Digital Technology and
Information Security at the Academy of the Ministry of Internal Affairs

Abstract
In this article, one of the most dangerous threats that are currently facing is cyberterrorism and the fight against it and on this, information about international experiments is presented. Several suggestions and recommendations to combat cyberterrorism have also been made.

Keywords: Cyber, cyberterrorism, analysis, terror, computer, crime, internet, logic bomb, virus.

Introduction

The growing development and expansion of the world spider web (internet (www)) is the reason for the emergence of cybercrime of various manifestations in this area, including crimes of a terrorist orientation. The current risks and threats, first of all, international terrorism, religious extremism, illegal migration, human trafficking, the growing spread of foreign ideas among our people among young people, set new tasks for the internal affairs bodies to prevent and end them in time.

Analysis of the growth of cyberterrorism suggests that its threat to humanity as a whole is increasing day by day. The reason is simple. Today there is no room left in the world where there is no computer penetration, competition among states to create fast internet consumption is reaching the latest peak.

We can cite cases of "breaking" into a computer, stealing and assimilating information within the network or in the system, embezzling citizens' personal funds from credit cards, sending dangerous viruses to the personal computers of large organizations or individuals, and electronically demanding funds as early stages of the functioning mechanism of cyberterrorism.

First, the fact that the mechanism of operation of this crime has not been fully and reasonably studied by international analysts;

Secondly, it is difficult to identify a terrorist inside the virtual world and secure it, in itself, the traces of cyberterror are almost invisible, unlike the existence in which we live.

Unfortunately, the "electronic world" is used as the main weapon for various political forces on the path of their terrorist, extremist propaganda and ideas, the promotion of their views to the public, the implementation of various criminal gang activities. The

Journal Zone Publishing, Ilford, United Kingdom

fact that large negative forces, creating their ideological space on the internet, are conducting a comprehensive informational terror – "cyber jihad" on the internet, new threats to global and regional security, creating problems, creates problems of ensuring information security in front of the countries of the world.

Like the major countries of the world, the Internet is entering Uzbekistan in fierce steps and has a place in our daily lives. Currently, the number of internet users in our area has exceeded twenty million. Today, terrorism is not limited to the territory of a particular state, where terrorists are hiding or their headquarters are located. They have already moved to the cyber world. Terrorist organizations masterfully use the latest capabilities of technology and the internet to expand their ranks and achieve their goals.

In national legislation, the relationship with combating terrorism is regulated in the law of the Republic of Uzbekistan PQ-167-II of December 15, 2000 “on Combating Terrorism”, in which terrorism (Article 155), information and facts about terrorist acts being prepared or committed are not reported (article 155), training for the purpose of carrying out terrorist activities, criminal liability for acts such as withdrawal or movement (art.155) and financing of terrorism (art. 155) is defined in the Criminal Code of the Republic of Uzbekistan. According to experts, the consequences of organized cyberterrorism using high technologies – nuclear, chemical or bacteriological cells-may be more dangerous.

The arsenal of computer terrorists today-various viruses, malware, “logical bombs”, that is, pre-installed in the program

and is made up of commands that can be run at the right time. However, so far, modern terrorists are using the internet mainly as a means of propaganda and information transmission, and not as a new weapon.

Unlike an ordinary terrorist, a cyberterrorist uses special programs designed to achieve its goals, such as modern Information Technology, Computer Systems and networks, unauthorized access to computer systems and remote attacks on the victim's information resources. For these purposes, they primarily use computer viruses that carry out the removal, modification or destruction of information on the network, including the aforementioned "logic bombs", "Trojan" programs, malware and other types of information weapons.

Cyberterrorism poses a serious threat to a country with a banking, transport and energy system, especially if the private sector of the government, state and economy relies on information networks and high technologies.

In our national legislation, the concept of cyberterrorism and its methods are practically not covered, this situation is one of the main problems in combating cyberterrorism and obtaining it. Even in national legal science, no single point of view has been developed regarding the definition of the concept of" cyberterrorism".

It should be noted that the term cyberterrorism is guessed for the first time

In the 1980s, it was used by Barry Colleen, a senior research fellow at the Institute for Security and Intelligence () in the United States.

Some scholars define the concept of cyberterrorism as its political, economic

Journal Zone Publishing, Ilford, United Kingdom

and in order to gain an advantage in solving social issues, the assassination of people, the implementation of destructive and a number of other actions towards material objects, the amendment of objective information is defined as a set of illegal actions aimed at awakening kurquv and wahhima in society through violation of the law, while others are used to deliberately commit information processed by a computer,
and to aim to provoke a military conflict in a provocative way - they describe.
Ronald Dick, director of the US fbq Center for national infrastructure development, in a 2002 report on the website of the khukumat organization, described cyberterrorism as a new manifestation of terrorism that uses computers and networks to achieve its goals and destroy state infrastructures, calling computer technology addiction the "Achilles point "("weak point"author's explanation) of the modern world.
Considering the concept of cyberterrorism, the main methods of its occurrence, as well as its importance and goals, we offer the following to solve the existing problems in this direction:
1. Actively conduct propaganda, creating channels in the media and social networks, posting commercials and various podcasts.
2. Organization and conduct of training courses for law enforcement officers. For example, the students of the University of the Republic of Uzbekistan will receive the necessary knowledge in this direction
and give skills.
3. In the structure of law enforcement agencies, it is advisable to establish units specializing in the fight against cyberterrorism. (For example, in the "Cyber Security Center"of the Ministry of internal affairs of the Republic of Uzbekistan).
4. Conducting scientific approaches based on the Prevention of cross-border terrorist cyber attacks and developing scientific and methodological support in this area, through which the development of a single platform that will be integrated into all countries and the continuous study and practical use of foreign experience.
In conclusion, cyberterrorism actions committed using high technologies in the 21st century can provoke a global information crisis, cause serious damage to the infrastructure of countries, confront different countries, and thereby directly endanger certain regions of the world. In the criminal law of the Republic of Uzbekistan, such cyberattacks should be given a decent response. Therefore, in the field of combating cyberterrorism, it is advisable to make criminal justice policy one of the priorities of improvement and create conditions for training in this field, becoming mature specialists and personnel.

References

1. https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/
2. https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure
3. Мороз Н. О. Деятельность Интерпола по координации сотрудничества в борьбе преступностью в сфере высоких технологий // Вестник Полоцкого государственного университета. Серия D: Экономические и юридические

Journal Zone Publishing, Ilford, United Kingdom

науки. 2011. № 14. С. 147.
4. Ўзбекистон Республикаси Жиноят Кодекси 155-моддаси - https://lex.uz/docs/111453
5. http://stopterror.uz/uz/publications/analytics/5414/

Journal Zone Publishing, Ilford, United Kingdom