УДК 343.3/.7

Serebrennikova A.V.
Doctor of law, Professor of criminal law and criminology
Moscow State University. M. V. Lomonosov
Russia, Moscow
DOI: 10.24411/2520-6990-2020-12048

CYBER TERRORISM: MODERN CHALLENGES

Abstract.
The article discusses the causes and conditions of the spread of the threat of cyber terrorism in the present and future. Describing cyberterrorism as a negative social phenomenon, the author makes an attempt to eliminate semantic contradictions regarding his concept. Analyzing the current situation in the international and domestic context, the author identifies the main causes and conditions for the spread of cyber terrorism, based on modern research in this area.

Key words: *cyber terrorism: cyber-attacks; the Internet; causes and conditions of crimes; national security; the Internet.*

Modern technological progress has led to increase in the equipment of organizations engaged in terrorist activities, as well as forms of manifestation of this negative social phenomenon. Use of information technology in the activities of terrorist organizations has become routine, setting law enforcement agencies with new tasks to counter it. This situation at the beginning of the XXI century led to the formation of a completely new type of criminal activity - cyber terrorism [3]. The dynamics of this type of crime is constantly growing, which is declared at the highest state level [4].

The process of formation of a clear and consistent definition of the term "cyber terrorism" has not yet been completed, since there are several significant contradictions in it. This is due to the fact that the discussion of cyber terrorism mostly occurs in the mass media, with a tendency for journalists to embellish and dramatize, rather than scientific accuracy and conciseness in the definition of new terms. In addition, the field of computer technology is replete with many similar terms formed by simply adding the prefix "cyber", "computer" or "information" before another word. Examples of such terms include: "cybercrime", "cyber terrorism", "cyber hacking", "cyber-attacks", "cyber tactics", "cyber-harassment", "computer war", "information war", "virtual" war ","‟ digital terrorism ". In one way or another, the above terms reflect the essence of a single phenomenon, referred to by some researchers as "new terrorism."

The first attempt to introduce it into the given terminology was made by an American researcher in the field of information technology Dorothy Denning in her numerous publications and in official statements [7].She presented cyber terrorism as a phenomenon bringing together cyberspace and terrorist activities. In the definition of cyber terrorism, Denning included attacks and threats of such attacks against computers, information networks and the content which they store. The main methods of cyber terrorism were identified as intimidation or coercion of public authorities or the population. The goals of cyber terrorism are similar to the goals of "traditional" terrorism and have a political or social implication. Cyber terrorism leads to violence against people or property, or causes fear.

In this regard, one should point out the differences between the concepts of "cyber terrorism" and "hacktivism", which is mostly used in the works of foreign researchers. In our opinion, "hacktivism" should be understood as anonymous actions carried out using information technology aimed at identifying, manipulating or otherwise using vulnerabilities in computer operating systems and other software. A distinctive feature of hacktivists before hackers is their political beliefs, which serve as the basis for their activities. The main methods used by hacktivists to achieve criminal goals are: virtual blockades, attacks by users of messaging and email services, hacking computers, computer viruses and worms.

One of the central problems studied by criminological science is the problem of determining the causal complex of crime formed by its causes and conditions. Let us consider in more detail the causes and conditions that contribute to the spread of cyber terrorism.

Of course, the first reason of development of cybercrime in general and cyberterrorism — in particular, is the virtually unlimited possibility of financing them from persons who have a political, mercenary, or other interest in achieving the goals of these crimes [1, p.53].

And, if before the revolution in the field of information technology, tracking such financial transactions was not difficult for law enforcement agencies, recently it has been a very laborious process. The anonymity of such operations attracts large organizations with extensive material resources, criminal groups and individuals, and even entire states [5, p.10].

Financing and material support of international terrorism from various sources are carried out with certain goals. Interest of transnational corporations in financing cyber terrorism consists in the fact that in this way they can eliminate competitors or make changes in the investment climate of the states in whose jurisdiction they operate. Interest of individual states in financing cyber terrorism is limited to solving certain political problems at the global and regional levels. Cyber terrorism is a tool for masking and legalizing criminal activity for the subjects of shadow economy [2. p,147]. The motives for financing cyber terrorism by private individuals may vary, but they serve an ideological

function by supporting and endorsing cyber-attacks [6, p.245].

Currently, when engaging in cyber terrorism, criminals are guided by various motives. However, the main ones are financial or political. Cyberterrorists are aware of the fact that modern state infrastructures are dependent on information and telecommunication networks and are actively using it for their own purposes. For example, Mohammed bin Ahmad al-Salim's article "39 Ways to Serve and Participate in Jihad" introduces the concept of "electronic jihad", which is considered as one of the ways to destabilize Western states [8. p,220].

The second reason of the spread of cyber terrorism is also of an economic nature and consists in its cheapness compared to "traditional" terrorist methods. Cyberterrorists do not need to purchase expensive equipment, weapons, explosives, special tools and supplies; for this distribution of information and malware, it is enough for them to have access to a personal computer with the Internet connection.

The third reason for the spread of cyber terrorism is its anonymity. Typically, cyber-terrorist individuals use pseudonyms or use guest access to resources that involve distribution of information or malware. This makes it very difficult for law enforcement agencies to search for and detect criminals. In addition, the barriers that exist in modern cyberspace (firewalls, brandmauers, etc.) often do not allow us to reliably establish the identity of network users, contrary to the physical barriers in real life (checkpoints for navigation, borders for crossing, etc.).

The fourth reason is the multitude of goals which cyberterrorism can achieve. Cyber-terrorists can carry out attacks on computers and information servers of governments, state bodies, individuals, utility facilities, infrastructure facilities of strategic importance, etc. The diversity and complexity of the potential targets of cyber terrorists ensures the possibility of finding weaknesses and vulnerabilities.

The fifth reason is the possibility of remote implementation of cyber terrorism. Cyberterrorism, compared to conventional forms of terrorism, requires less physical and psychological preparation, risk of death and travel, which makes it easier for terrorist organizations to engage more and more new supporters in their activities.

And finally, the last reason of the spread of cyber terrorism is the wide coverage of an almost unlimited public. Capabilities of modern information and telecommunication systems allow cyber-terrorists to spread their ideology in a very short time for millions of users before such information is identified by law enforcement agencies and blocked.

Summing up the present study, we note that the correct understanding of the causes and conditions for commission of cyberterrorist crimes allows law enforcement agencies to successfully counteract terrorists and persons supporting such activities. The successful implementation of programs to combat cyber terrorism is possible only with the close cooperation of states.

List of cited references

1. Antonian E.A.. Issues of implementing new technologies to counteract cyberterrorism // Monitoring of law enforcement. 2020. No. 1 (34). P. 51-55.

2. Baturina E.V. Information-analytical system for monitoring shadow cashless cash flow: basic elements, author's modeling algorithm // University Herald. 2019. No. 7. P. 144-151.

3. Glotina I.M. Information terrorism and its impact on the economy // PSE. 2014. No.3 (51). URL: https://cyberleninka.ru/article/n/informatsionnyy-terrorizm-i-ego-vliyanie-na-ekonomiku (Accessed date: 08.07.2020).

4. Mishustin announced the increase in the activity of cybercriminals [Electronic resource] // Access: https://www.gazeta.ru/tech/news/2020/07/08/n_14643169.shtml (Accessed date: 08.07.2020).

5. Panenkov A.A. System of crimes in the field of computer information belonging to the structure of terrorist activities (cyber terrorism) as a real threat to the external and internal contours of the national security of Russia // Military and Law Journal. 2014. No. 4. P. 3-13.

6. Chernov S.A., A.M. Shunayev. Threats to the economic security of the Russian Federation in the information field // In the collection: State and business. Ecosystem of the digital economy. Materials of the XI International Scientific and Practical Conference. North-West Institute of Management, RANEPA under the President of the Russian Federation. 2019. P.243-246.

7. Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", Global Problem of Solving Information Technology and Tools, December 10, 1999, https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

8. Holt, Thomas J.; Freilich, Joshua D.; Chermak, Steven M. (2017). "Exploring the Subculture of Ideologically Motivated Cyber-Attackers". Journal of Contemporary Criminal Justice. 33 (3): 212–233. doi:10.1177/1043986217699100.