CYBERTERRORISM IN BALTIC STATES

Zinchenko O.I.
V.N. Karazin National University, Kharkiv, Ukraine

Summary. The article is devoted to the problems of combating cyberterrorism and cybercrime in the Baltic States. The nature of cyberterrorism in these countries features and ways to overcome it have been determined. The current state of cyberterrorism in the Baltic States and the existing forms of combating this phenomenon are studied.

Keywords: cyberterrorism, fight against cyberterrorism, Baltic countries, Latvia, Lithuania, Estonia.

Not the only, but one of the important components of national information security is security in the field of the global information and telecommunications network Internet.

Unlike classical offenses, usually committed in a specific place in space, offenses committed using the global information and telecommunications network Internet are sometimes not only not tied to a specific geographic point, but it is also impossible to determine in which state they were committed.

Today we can say that the Internet covers all countries of the world, since with the use of new technologies (the use of mobile satellite communication devices), it is possible to connect to the Internet from anywhere in the world. If we talk about the deployed infrastructure, then in this context, the Internet today covers more than 150 countries of the world [1].

Recently, free Wi-Fi Internet access points have become more and more popular, which allows an offender to connect to the Internet anonymously, often leaving virtually no traces. Persons with sufficient knowledge in the field of information and telecommunication technologies and having sufficient experience in their application actively use various technologies to disguise and/or falsify their identity, thus avoiding punishment for illegal actions.

At the same time, domestic legislation, as well as the legislation of many foreign countries, lags behind the speed of development of information technologies and does not provide law enforcement officers, justice officials and others with sufficient legal tools to ensure the proper level of legality and law and order, as well as to promptly investigate offenses and the involvement of criminals to legal and fair responsibility.

Meanwhile, commercial companies, non-profit, state and municipal organizations and institutions, international organizations, and public organizations face even greater threats. Offenders often gain unauthorized access to their networks, servers, websites, accounts with impunity, which, in turn, entails unauthorized access to information (including reading, changing, deleting), stealing personal data from clients, obtaining information constituting a commercial secret or know-how, embezzlement of funds, damages the image and leads to irrecoverable loss of lost profits.
State and local government bodies are sometimes even more exposed to cybercriminals and cyberterrorists who organize theft of data from state information systems and / or prevent their normal operation. As an example, «one of the first such cyber wars occurred in April 2007, when, in connection with the decision of the Estonian government to move the monument to the Liberator Soldier, the websites of the state structures of this country were subjected to organized attacks. This blow became extremely painful due to the presence in Estonia of a developed system of the so-called electronic state, to which not only European, but also leading Asian countries are so actively striving to switch. Thanks to her, most of the state office work in this Baltic country is conducted electronically: government meetings are broadcast via the internet, here you can fill out a passport application form, pay utility bills and even vote ...» [6].

Computer terrorism (cyber terrorism) should be understood as intimidation of the population and authorities in order to achieve criminal intentions. This manifests itself in the threat of violence, maintaining a state of constant fear in order to achieve certain political or other goals, coercion into certain actions, drawing attention to the identity of the cyber terrorist or terrorist organization he represents. Causing or threatening to do harm is a kind of warning about the possibility of causing more serious consequences if the conditions of the cyber terrorist are not met.

Proponents of the second approach believe that cyberterrorism is a type of terrorism, which is based on the method of committing terrorist acts, which arose in the development of information and telecommunications technologies and their introduction into all spheres of modern society [2; 7]. For example, Dorothy Denning (an expert at the US Center for Terrorism Research) defines cyberterrorism as an element of the classification of terrorist activities on the Internet and presents it as computer attacks designed to cause maximum damage to vital information infrastructure [8].

Terrorism researchers have a different view of the nature of cyberterrorism. They believe that cyberterrorism manifests itself in two forms:

- first, computer economic crimes committed with the help of hacker specialists, including:
  1) machinations and manipulations of data processing systems (unauthorized transfer of money and their use);
  2) espionage (penetration into confidential communication channels of state bodies for obtaining information, espionage for the purpose of obtaining information on closed technologies);
  3) sabotage (damage to hardware and software by viruses that disrupt the functioning of government agencies and other institutions);
  4) illegal use of computer services (programs, purchases at the expense of others, etc.);
- secondly, the disclosure of secrets - obtaining commercial and confidential information (which is inextricably linked to the first type), including:
  1) unauthorized receipt of information for its misuse by persons who do not have appropriate access;
  2) illegal collection and hiding of information;
  3) violation of the rules for the use of confidential information [3, p. 203-211].
Means of implementation can be extremely diverse and contain all types of modern information weapons. In this case, the effectiveness of information weapons is compared with weapons of mass destruction [5]. Thus, according to the International Policy Institute for Counter Terrorism, terrorists already use cyber weapons such as computer viruses, «worms», «Trojan horses», «logic bombs» and other hacking tools. However, today the most popular and visible type of cyberterrorism is hacking and posting slogans and appeals. For example, in May of this year, the website of the President of the Russian Federation was hacked from the servers of the Baltic States. In turn, Estonian government sites were attacked by hackers from Russia, as a result of which NATO representatives sent anti-hacker specialists to Estonia to investigate these attacks on servers.

Along with such means of destroying information computer systems as computer viruses, software embedded devices should be noted means of suppressing information exchange in telecommunications networks, its falsification, transmission through public and private information management channels and tools to implement software bookmarks in public and corporate information systems and manage them remotely. Such tools include, for example, the neutralizer of test programs, which ensures the impossibility of detecting natural and artificial defects of software by special test programs [4, p. 119].

In addition, cyber terrorism is a serious threat to humanity, comparable to nuclear, bacteriological and chemical weapons, and the extent of this threat, due to its novelty, has not yet been fully understood and studied. The experience that the world community already has in this area clearly testifies to the undoubted vulnerability of any state, especially since cyber terrorism has no state borders, a cyber terrorist is capable of equally threatening information systems located almost anywhere in the world. It is very difficult to detect and neutralize a virtual terrorist due to too few traces left by him, in contrast to the real world, where there are still more traces of what he has done.

Also in 2020, the Netherlands, the Baltic republics and several Eastern European countries decided to stand guard over Europe's cybersecurity. The countries are ready to sign an agreement on the creation of the European Union's Cyber Rapid Response Force. By the way, this project was approved back in 2017 by the participants of the European program of Permanent Structural Cooperation (PESCO). As a result, the signatures in the memorandum were put by representatives of Poland, Croatia, Romania, the Netherlands, Lithuania and Estonia.

According to this document, the International Rapid Response Group will constantly be on duty in various locations and will be able to resist a cyberattack at any time. The newly formed civil-military groups of the six countries will participate not only in the virtual, but also, if necessary, in the physical stages of the investigation of major incidents. In accordance with the agreement, international teams will be in reserve in different countries, ready to respond to a cyberattack.

It should be admitted that hacker attacks and cybersecurity issues in general today are indeed a very topical issue for many countries of the world. Only few of them are ready to cooperate in this area.

Cybersecurity experts say that in order to truly combat such a threat, the work of a global organization like the UN is necessary. Only then, in technical terms, it will be possible to talk about a real fight against cybercrime. All countries should:
1) first, agree on who, for example, they will recognize as cyber terrorists;
2) secondly, it is necessary to prohibit their activities legally. When at least two of these points are recognized by all states, hacker attacks, telephone terrorism and virtual attacks on critical infrastructure can already be effectively suppressed.

But the hackers who attack these six countries will simply move geographically all the time to places where rapid response teams have no authority and no «target capture» tools.

For example, Estonia, Poland, the Netherlands, Romania, Croatia, and Lithuania have identified a group of hackers by tracing them to some route trace address located in another country. Of course, they will ask that country to grant them access to their data. And it will take a very long time. After all, states do not allow simply monitoring their information field.

In conclusion, we note that, first, thanks to the achievements of science and technology, information weapons are created and modernized, which can be used by terrorists to achieve their goals. Through the media (including digital television) and the global information network the Internet, terrorists have the opportunity to widely inform the public about their intentions. That is, terrorism acquires new features and reaches a new man-made and organizational level; secondly, given the trend of development of information and telecommunication technologies and opportunities for free access to them by a wide range of people, the danger of cyberterrorism is increasing. In turn, the role of information security, due to the growing threat of the use of information weapons in the global information circulation, is constantly growing; third: computer terrorism can not only localize or neutralize the activities of objects or groups of objects built on the functioning of information and telecommunications technologies, but also create a systemic crisis in those societies where the infrastructure of information circulation is widely developed.

At present, for the Baltic States, cyberterrorism has not moved from a «potential» threat to a «real» threat, so preventive measures should be taken to prevent its emergence. After all, these countries have already suffered significant damage from cyberterrorism. This necessitates an urgent solution to the problem, and the basis for combating cyberterrorism is to create an effective system of measures to prevent, detect and stop this type of activity.

References: