International Journal of Science, Technology and Society
2022; 10(2): 23-26
http://www.sciencepublishinggroup.com/j/ijsts
doi: 10.11648/j.ijsts.20221002.11
ISSN: 2330-7412 (Print); ISSN: 2330-7420 (Online)

Cyberattacks as a Tool of Destructive Influence of Cyberterrorism

Oleksandra Zinchenko

Department of Political Science, School of Philosophy, V. N. Karazin National University, Kharkiv, Ukraine

Email address:
alekca.98@ukr.net

To cite this article:
Oleksandra Zinchenko. Cyberattacks as a Tool of Destructive Influence of Cyberterrorism. *International Journal of Science, Technology and Society*. Vol. 10, No. 2, 2022, pp. 23-26. doi: 10.11648/j.ijsts.20221002.11

Received: December 9, 2021; **Accepted**: January 4, 2022; **Published**: March 4, 2022

Abstract: The article is devoted to the concept of "cyberterrorism", which originates in the recent past and it is derived from the broader general concept of "terrorism" and defines a global threat to information security. The article also explains how cyberterrorism interferes with the normal functioning of institutions and public authorities. Actually, based on all the above, it can be noted that cyberterrorism is a very complex and multifaceted phenomenon, which has a diverse structure, which complicates the development of methods to combat and prevent it. Modern society has yet to develop an effective system to counter and combat this information evil of today. Today, the issue of combating cyberterrorism remains open, because due to the novelty and incomplete understanding of the danger of the phenomenon, as well as the impossibility of developing a single definition, countries can not comprehensively protect themselves from cyberterrorist attacks. However, a number of issues remains open, including the lack of a legal single concept of "cyberterrorism" in most European countries and a system of clear mechanisms to combat cyberterrorism at the regional and national levels. Therefore, the urgency of this problem is very acute, as the latest technology allows terrorists to expand their activities. These issues require urgent solutions both domestically and globally. Effective international cooperation in the prevention and elimination of the consequences of cyber terrorism is essential.

Keywords: Cyberattack, Cyberterrorism, Information Security, Modern Technologies

1. Introduction

Today, when it comes to total informatization and computerization, when all systems of life have come under virtual control, ensuring the security of both individuals and the state as a whole is becoming increasingly difficult.

2. The New Phenomenon

2.1. What Does It Mean

In the twentieth and twenty-first centuries, views on the main subject and the object of security have changed. If before the main objects of protection were the territory, state system, sovereignty, and states tried to protect themselves from terrorist attacks, by creating and maintaining law enforcement agencies, which were the main guarantor of security, then at the turn of the century modernizing the information sphere, and Terrorist attacks are increasingly moving into cyberspace, a radically new phenomenon has emerged, called "cyberterrorism", which is becoming increasingly difficult to resist and requires modernized means of protection and counteraction.

The real manifestation of cyberterrorism is carried out through cyber attacks on information resources of both individual spheres of human life and states as a whole.

The concept of "cyberterrorism" originates in the recent past, it is derived from the broader general concept of "terrorism" and defines a global threat to information security.

In general, cyberterrorism, as a dangerous phenomenon, began to emerge in the 70's of XX century in the form of cybercrime, namely the beginning of the first cyberterrorist acts is a crime committed in 1973, when the cashier of New York "CITY BANK" using a computer, transferred to his account $2 million. It is believed that this is where the official history of cybercrime and cyberterrorism, as their worst manifestation, begins [1].

2.2. The Historical Background

In 1981, the scale of cybercrime began to gain momentum, so hacker Ian Murphy, known as Captain Zap, was the first to be found guilty of committing cybercrime. He broke into the network of the telephone company AT&T and changed the program of call charging, after which it became possible to conduct daytime telephone calls at night and vice versa. The court sentenced him to 1,000 hours of community service and 2.5 years probation [2].

Later, in 1983, the first so-called "virtual criminals" were arrested - a group of hackers called "Gang 414" in Milwaukee, Wisconsin, USA. Hackers hacked 60 computers, some of which belonged to the Los Alamos National Laboratory in New Mexico [3].

Not having at that time a detailed definition and signs of criminal activity in the information space, law enforcement agencies were faced with the fact that such signs contained terrorist activity familiar to all. Meanwhile, the method of its implementation and the so-called tools used were different. It was necessary to react immediately and reconsider the approaches to combating such phenomena, as they posed an even greater threat to the interests protected by the relevant legal systems. It was these attacks that actually started the phenomenon of cyberterrorism.

3. The Definition

3.1. What Did Some Experts Say

However, at that time we were not talking about cyberterrorism as such, because the term "cyberterrorism" appeared only in the mid-80's of the XX century, and was proposed by a senior researcher at the American Institute of Security and Intelligence Barry Collin, who used it in the context of the trend towards terrorism from physical to virtual.

For example, Barry Collin defined it as follows: “Cyberterrorism is deliberately destructive activity, or threats to computers and / or networks, with the intent to harm or further social, ideological, religious, political consequences or other purposes, or to intimidate any what person in order to promote such goals" [4].

Thus, a radically new concept is being introduced in the world, which characterizes a much new criminal activity, which now has no boundaries, but has an extreme degree of danger.

3.2. Transformation

The first decade of the 21st century ushered in the cultural transformation of terrorism as new technologies, such as computers and networks, became available as a means of exploitation.

The current increase in cyber-attacks may represent a new generation of "terrorists" and their dissatisfaction with governments, private companies or other non-governmental groups. The use of cyber technology has many benefits for the user and the potential for more key damage than a bomb is growing daily. If earlier actions of cyberterrorism were carried out by separate groups of hackers, now the targets of the state which finance the cyberwarts and develop modern cyberweapons are involved in cyberattacks. As a result, cyberterrorism is becoming an effective way to put pressure on the authorities.

Cyberterrorism uses the openness of the Internet to discredit governments and states, host terrorist sites, damage and destroy key critical state infrastructure systems, by falsifying data, or by regularly removing these systems from service. In addition, cyberterrorists can exert ideological, political, economic or organizational influence on the assessment, opinion and behavior of certain segments of the population of a country via the Internet. Based on the fact that it is currently impossible to control or restrict access to information resources of the Internet of information consumers, the potential criminogenicity of this information and communication resource increases sharply.

Thus, terrorist organizations are increasingly using new information technologies and the Internet with the criminal intent to obtain funds, carry out propaganda or transmit classified information.

And the Internet, in turn, is the main weapon of terrorist groups, which they use for communication, propaganda, dissemination of information, viruses and more [5].

3.3. The Variety

The main form of cyberterrorism is cyberattacks on computer information, computer systems, data transmission equipment, and other components of the information infrastructure, which are carried out by groups or individuals. Such attacks allow to penetrate into the attacked system, to intercept management or to destroy means of a network information exchange, to carry out other destructive actions. The effectiveness of forms and methods of cyberterrorism depends on the characteristics of the information infrastructure and the degree of its security [6].

Thus, the development of cyberterrorism threatens the security of the individual, society and the state at all levels of life. In the context of the development of the information society, cyberterrorism has long outgrown the regional and / or national scale. According to experts, in the future cyberattacks will include damage to the defense systems of states and even causing death to the population by undermining the work of important infrastructure measures [7].

Examining these cyberattacks, it can be determined that such attacks should be divided according to the object of encroachment, ie they caused real physical harm to a person or serious violations of state infrastructure. Therefore, it is possible to identify such ways of carrying out cyberterrorist attacks as:

a) the use of computer technology to place in the network information that can affect people in order to sow fear [8]. For example, posting terrorist videos on the Internet - resources. The content of such videos is pursued by

such goals as propaganda of terrorism, incitement to hatred and hatred on the principle of nationality, religion, etc., warnings about planned or committed terrorist attacks, etc. Such videos serve as a lever of pressure on society and the state, panic. authority of state power;

b) recruitment and involvement of citizens in terrorist communities via the Internet. As the Internet has increased anonymity, it is not difficult to find a potential participant and recruit him to a terrorist organization. With the use of the Internet, the preparation of terrorist operations is organized, briefing is carried out with direct executors, tactical tasks are solved during terrorist attacks. In a similar way, terrorist financing, action planning and communication between members of such a criminal group, the acquisition of weapons and other ammunition [9];

c) criminal encroachment on computer infrastructure and information networks. Experts include, for example, the decommissioning of information systems, which will lead to the uncontrolled operation of affected facilities (which is especially dangerous in nuclear and chemical plants, as well as in the military for defense and attack systems) or the organization of destructive attacks (destruction information resources and lines of communication or physical destruction of structures that include information systems) [10].

This classification shows that network terrorists can be equally attacked by states, international organizations, large corporations and relatively small companies, politicians and other celebrities, as well as randomly selected people, and cyber-terrorist actions can be directed at civilian infrastructure. and military purpose.

We believe that the energy and telecommunications industries, aviation control centers, and financial institutions that are part of the state's defense complex are more attractive for terrorist cyberattacks. The targets of such attacks may be equipment, network protocols for data transmission, where information is stored, specific specialists in the field of information technology and service personnel. If the attacked objects are part of critical life support systems, outside interference in their work can lead to both large-scale destruction and human casualties.

3.4. The Ways of Comitting

So, we note that analyzing the history of cyberterrorism, the most common ways of committing cyberattacks include:

a) causing material and economic damage by breaking the security system, disrupting the operation or complete disconnection of means of communication, supply, public transport and military facilities;

b) providing psychological influence on the masses in order to destabilize the situation and spread chaos;

c) providing psychophysiological influence on certain social groups, as well as people involved in the information sphere;

d) providing provocative disinformation in order to upset the balance of power in the international arena, inciting military, ethnic and religious conflicts;

e) agitation and propaganda of radical and extremist ideas, recruitment of new members to existing terrorist organizations;

f) misinformation of law enforcement agencies of a particular state about alleged explosive devices planted on its territory, as well as about acts of terrorism being prepared, etc.;

g) influencing the decision-making of the authorities by threatening to commit a terrorist act;

h) disclosure and threat of publication or only publication of confidential information about the functioning of the information infrastructure of the state, socially significant and military information systems, encryption codes, the principles of encryption systems, etc.

In the event of such attacks, criminals mainly carry out actions aimed at destroying communications, damaging information and transport channels, using the latest developments in information technology to maintain communication, address organizational and financial issues, plan operations and monitor their implementation.

XXI century. characterized by a sharp increase in cyberattacks on the vital systems of states around the world. Their consequences are no less dangerous than physical attacks on critical infrastructure. Such cyber-based attacks can disrupt critical systems such as water and energy, nuclear reactors, transportation hubs, and other strategic facilities. For modern terrorists, the use of cyberspace is attractive because cyber-terrorist attacks do not require large finances, only the Internet, software, viruses and a PC connected to the network.

3.5. Types of Cyberterrorism

After analyzing the current manifestations of cyberterrorism, we can change that now the following types of cyberterrorism:

a) Simple - unstructured (attacks against information systems, usually using programs created by someone else (not the cyberterrorists themselves). This is usually the simplest type of attack, the losses from it are either minimal or insignificant

b) Advanced - Structured (the ability to conduct more complex attacks against multiple systems or networks and possibly modify or create basic hacking tools)

c) Comprehensive - coordinated (the ability to coordinate an attack, capable of causing massive disruption of the country's security systems. The ability to create complex hacking tools.

d) They have a strict structure, often represent organizations that are able to soberly analyze their actions, make some plans for attacks, and so on) [11].

This classification was proposed according to the version of "Monterey", and in our opinion fully corresponds to the current state of cyberattacks and correctly determines their typology.

4. Conclusion

Note that the threat of cyberterrorism is huge, and in some cases, its consequences can be irreversible. Modern society has yet to develop an effective system to counter and combat this information evil of today.

Thus, based on all the above, it can be noted that cyberterrorism is a very complex and multifaceted phenomenon, which has a diverse structure, which complicates the development of methods to combat and prevent it.

References

[1] Hnatyuk SO Cyberterrorism: history of development, modern tendencies and countermeasures. Information security. 2013. T. 19, № 2. S. 118–129.

[2] Murphy Ian A. Captain Zap. Hack Story. URL: https://hackstory.net/Captain_Zap.

[3] Dubov D. Approaches to the formation of a thesaurus in the field of cybersecurity. Political management. 2010. № 4. S. 19–30.

[4] Barry C. Future of Cyberterrorism: The Physical and Virtual Worlds Converge. Crime and Justice International. 1997. Vol. 13. Issue 2. P. 15–18. URL: http://www.crime-research.org/library/Cyberter.htm.

[5] Cyberterrorism as a part of modern problems of national security. URL: www.nbuv.gov.ua/ejournals/FP/2010-2/10bovpnb.pdf (access date: 12.09.2020).

[6] Andrew Conry-Murray. Security policy in times of terror. URL: http://www.osp.ru/lan/2002/02/083.htm.

[7] Cyberterrorism and personal data protection. LLC SIDCON Consulting Company, 2013. URL: http://people2people.com.ua/nashi-novosti/105-kiber-terrorizm-zaschita-personalnyh-dannyh.html.

[8] Kapitonova EA Features of cyberterrorism as a new type of terrorist act. News of higher educational institutions. Volga region. Issue. 2 (34). 2015 - P. 29-41.

[9] Kostikhin AA The Internet as a tool of terrorist and extremist organizations in psychological warfare. URL: http://www.iimes.ru/?p=4737.

[10] Mazurov, VA Cyberterrorism: concept, problems of counteraction. TUSUR reports. - 2010. Issue. 1. pp. 41-45.

[11] Golubev VA Cyberterrorism as a new form of terrorism. Computer Crime Research Center URL: http://www.crime-research.org/library/Gol_tem3.htm.