CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org

Volume: 03 Issue: 11 | Nov 2022 ISSN: 2660-5309

Cyberterrorism as a Threat to International Security

Rakhimov Mukhammadsodiq Davrjon ogli
Independent investigator of academy of the ministry of internal affairs, Tashkent, Uzbekistan

Abstract

This article analyzes the emergence and types of threats of cyberterrorism. Also, some examples show the fact that today the prevention of threats of cyberterrorism in ensuring the security of the world community remains relevant. In addition, the article noted the consequences of cyberterrorism cause great material and moral damage to people and government agencies.

ARTICLEINFO

Article history:
Received 6 Sep 2022
Revised form 5 Oct 2022
Accepted 29 Nov 2022

Key words: *cyber terror, internet, website, social networks, cyber fear, cyber-attacks, hacker, cyber security, terrorist organization.*

---***---

Introduction

We live in the era of the information society, when computers and telecommunications systems cover all spheres of human and state life - from solving problems of national security, healthcare and transport management to trade, finance, and even just interpersonal communication. Man has always been vulnerable, but recently we have learned that we are doubly defenseless - not only in real life, but also in a world that we knew nothing about three decades ago - the virtual world, cyberspace, the world simulated by computers. Society has taken advantage of telecommunications and global computer networks without foreseeing the opportunities for abuse these technologies create[1].

Results and its discussion.

Today, not only people, but entire states can become victims of criminals operating in the virtual space. At the same time, the security of thousands of users may be dependent on several criminals. The number of crimes and terrorism committed in cyberspace is growing in proportion to the number of users of computer networks, and, according to Interpol, the growth rate of crime, for example, on the global Internet, is the fastest on the planet[2]. At present, one can trace the increase in the number of Internet users, both around the world and in the Republic of Uzbekistan.

According to a global study by the analytical company WebCanape, the number of Internet users in the world is currently more than 4.66 billion people. In 2021, the number of websites on the Internet amounted to more than 1.9 billion. According to the State Committee for Communications, Informatization and Telecommunication Technologies of the Republic of Uzbekistan, Internet users in Uzbekistan increased by

[1] Тропина Т.Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Сборник научных трудов международной конференции "Информационные технологии и безопасность". Выпуск 3. – Киев: Национальная академия наук Украины, 2003. – С. 173 – 181.
[2] Номоконов В. А. Интернет и преступность: криминологические и правовые аспекты взаимосвязи // Организованный терроризм и организованная преступность. М., 2002. С. 187

27.2 million in the first quarter of 2021. Currently, the Internet is a favorable space for terrorist organizations, through which people can be feared.

Experts note that the World Wide Web attracts with the possibility of free access, low cost of communication, lack of censorship and other forms of state control, anonymity (which is most important), fast information transfer, large audience and technical capabilities.

Today, almost all active terrorist organizations have their websites, and some even have more than one website and in several languages.

It should also be noted that these sites contain manuals for making bombs, weapons and organizing terrorist attacks. Website owners usually get away with claiming that they are not the authors of the manuals and that they do not encourage the use of this information in practice.

In addition, psychological attacks are used to influence people, which consist in the distribution of threats aimed at sowing fear and a sense of helplessness, the dissemination of horrific images of their actions, such as the video of the murder of American journalist Daniel Pearl by the people who captured him, posted on several websites.

It is worth noting that terrorist organizations have recently given priority to the Internet when discussing their plans, exchanging information, conducting propaganda and recruiting new members.

Thus, in 2006, the leadership of the radical Iranian organization Ansar e-Hezbollah announced the creation of a website (www.ansaronline.com), where those who wish could register and take part in the attack on US facilities in the event of strikes on Iran.

Similarly, on the Internet site of the radical extremist organization "Hizb ut-Tahrir" (http://www.hizb-ut-tahrir.org), information was disseminated regarding the ideology and direction of this organization. The study of individual articles indicates that some of them contain calls for the so-called "jihad" and building a "caliphate" on the territory of Central Asia.

As former CIA director M. Hayden noted, the US intelligence agencies received information that Al-Qaeda in European countries is trying to convert Europeans to Islam, who, because of their appearance, do not arouse suspicion, in order to further prepare them for terrorist attacks. At the same time, this process is carried out with the help of the so-called. "Correspondence terrorist university" on the Internet[3].

According to Western experts, there are currently about 5,000 sites on the Internet that are directly used by terrorists to carry out not only ideological work, but also training and recruiting new members into their ranks[4].

At the same time, it is necessary to note the widespread increase in the number and scale of damage caused by criminal groups operating in cyberspace.

According to the experts of the Council of Europe, the losses from cyber-attacks and viruses amount to about 12 billion a year, and the violation of property rights causes damage of 250 billion dollars to the European Union[5].

In turn, according to the research service of the US Congress, the damage to firms caused by electronic hackers annually amounts to 226 billion dollars a year.

Massive power outages in Brazil on September 26-27, 2007, when more than 3 million people were left without electricity in several dozen cities, turned out to be the result of a targeted attack by cyberterrorists[6].

[3] «Аль-Каида» тренирует боевиков с «западной» внешностью для терактов в США (30.03.2008) (http://i-r-p.ru/page/stream-event/index-19151.html)
[4] Институт религии и политики (28.03.2008) (http://i-r-p.ru/page/stream-event/index-19103.html)
[5] Центр исследования проблем компьютерной преступности. В. Голубев к.ю.н.,доцент. Кибертерроризм как новая форма терроризма (www.crime-research.org)
[6] Хакеры оставили без электричества 3 млн. бразильцев (www.securitylab/news/tags/)

At the same time, according to information distributed by the Associated Press on July 4, 2009, the network representations of the US Federal Trade Commission, the Department of the Treasury and the Department of Transportation, as well as the secret service responsible for the security of the first persons of the state, were subjected to a hacker attack and were disabled on few hours[7].

According to the analysis of Kaspersky Lab, which develops anti-virus programs, in 2008, 23,680,646 attacks were recorded using new types of viruses that could disable computer systems. In turn, in 2009 the number of malicious programs was 73,619,7671[8].

In recent years, the emergence of cyberterrorism and highly publicized crimes committed by international criminal groups indicate that cybercrime has become transnational.

The alarming fact is that with the development of the Internet, not only international cyber-attacks, but also the mistakes of professionals can have serious consequences. For example, in 1997, a mistake by an employee at Network Solutions caused all sites with addresses ending in ".net" or ".com" to become inaccessible. That is, negligence on the part of only one person disrupted the operation of the entire World Wide Web.

At the same time, cyber-attacks are becoming a means to achieve political goals. A typical example is a web-based denial-of-service attack: attackers simultaneously access a site, connect to a server, send emails, or post on forums to make it difficult or even impossible for other users to access the site.

Such a website or server becomes overloaded with requests, which leads to interruptions in its operation or to its complete cessation. The first attack of its kind was carried out by a group calling itself the Strano Network, which was protesting against the French government's nuclear and social policies. On December 21, 1995, this group attacked the websites of various government agencies for an hour. Group members from different continents were instructed as follows: they were supposed to, all at the same time, use browsers to access government sites. As a result, some sites were indeed unavailable for some time[9].

The transnational aspects of cyberterrorism are becoming increasingly apparent. The Kosovo conflict is considered the first Internet war, during which various groups of computer activists used the Internet to express their condemnation of the actions of both Yugoslavia and NATO by disrupting government computer systems and gaining control of websites, followed by distortion their appearance (the so-called "deface site").

In parallel, stories about the dangers and horrors of war circulated on the Internet, and politicians and public figures used the Internet to reach the widest possible audience around the world with their appeals[10].

It should be noted that today almost any military or political conflict is accompanied by an organized confrontation on the Internet. For example, in 2005, a new school history textbook was published in Japan containing a distorted account of events in China in the 1930s and 1940s that did not address the war crimes committed by Japanese forces during this intervention, which caused a whole wave of cyber-attacks. The targets of these attacks were Japanese ministries and government agencies, websites of large Japanese corporations, and websites dedicated to World War II.

[7] По материалам пресс-релиза компании Cisco Systems www.mis.ru

[8] Исмоилов О.М. “Обеспечение информационной безопасности государственных органов Республики Узбекистан в телекоммуникационных сетях на современном этапе“ Диссертация на соискание степени магистра политических наук ВШСАП РУ, Ташкент, - 2010 г С. - 14

[9] Деннинг Д. «Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику» («Activity, Hactivity and Cyberterrorism: The Internet as a Means of Influence on Foreign Policy»). Владивостокский центр исследования организованной преступности, перевод Т.Л. Тропиной http://www.crime.vl.ru/index.php?p=1114&more=1&c=1&tb=1&pb=1

[10] Андреев А., Давыдович С. «Об информационном противоборстве в ходе вооруженного конфликта в Косово», Центр практической психологии «ПСИ-ФАКТОР» http://www.psyfactor.org/warkosovo.htm

In this case, the Chinese hackers showed a high degree of organization, manifested in the synchronicity and mass nature of their attacks. Given that the Internet is controlled by the state in China, it is assumed that this attack was authorized by the Chinese government.

The example of China was copied by Russian hackers who carried out several DDoS (distributed denial of service) attacks.

Over the course of several days in late April and early May 2007, Estonian government websites were attacked. The Nashi youth movement claimed responsibility for these attacks[11].

According to some reports, today there are more than 5 thousand websites created and maintained by organizations that the international community has recognized as terrorist - among them Iraqi militants, al-Qaeda and Chechen separatists. Some of them are created in many popular languages at once, creating a massive source of propaganda. The Internet offers terrorist groups an unprecedented level of direct control over the content of their messages. This greatly increases their ability to shape the perception of a different target audience, and manipulate not only their own image, but also the image of their enemies.

It should be noted that many countries fight terrorism by informing. Terrorists use false information to recruit. The civilian population should be informed in order to know what terrorism is, how it manifests itself on the Internet, what sites exist, what their purpose is, what the participation in such groups leads to, and so on. A person who knows and is aware is not so easily led astray.

In addition, terrorists can attack or break into the computer systems of various institutions. The consequences of this can be varied: the military, intelligence, medical services, transport and financial systems, etc. may suffer. The potential scale of cyberterrorism is horrendous, as it can wreak havoc on not only government but also commercial structures, paralyzing, for example, banking operations. Cyberterrorists can also launch psychological attacks through cyberterrorism, more specifically, creating fears of the threat of such acts. “Cyber fear” arises from the concern about the threat of computer attacks (for example, plane crashes, disruption of air traffic control systems, disruption of the national economy system by disrupting the computer systems that regulate stock exchanges, etc.), which increases so much that society begins to believe that an attack will happen.

This is not the first time that the issue of using the Internet for terrorist purposes has been raised. For example, in September 2012, the Australian Department of Defense released a report that revealed that members of the Taliban were creating fake Facebook pages with photos of attractive women. With their help, the Islamists extract information from the soldiers.

Conclusion.

Based on the foregoing, it can be assumed that cyberterrorism today is a new type of threat to national security, which requires special countermeasures.

With the rapid pace of development of cyberterrorism, it can be assumed that the failure to take tough measures to counteract cyberterrorism, given its psychological and technical aspects by the governments of the world, can lead to a decrease in the level of state security and a tendency to instill panic in society.

References:

1. Тропина Т.Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Сборник научных трудов международной конференции "Информационные технологии и безопасность". Выпуск 3. – Киев: Национальная академия наук Украины, 2003. – С. 173 – 181.
2. Номоконов В. А. Интернет и преступность: криминологические и правовые аспекты взаимосвязи // Организованный терроризм и организованная преступность. М., 2002. С. 187

[11] Андреев А., Давыдович С. «Об информационном противоборстве в ходе вооруженного конфликта в Косово», Центр практической психологии «ПСИ-ФАКТОР» http://www.psyfactor.org/warkosovo.htm

3. «Аль-Каида» тренирует боевиков с «западной» внешностью для терактов в США (30.03.2008) (http://i-r-p.ru/page/stream-event/index-19151.html)
4. Институт религии и политики (28.03.2008) (http://i-r-p.ru/page/stream-event/index-19103.html)
5. Центр исследования проблем компьютерной преступности. В. Голубев к.ю.н.,доцент.
6. Кибертерроризм как новая форма терроризма (www.crime-research.org)
7. Хакеры оставили без электричества 3 млн. бразильцев (www.securitylab/news/tags/)
8. По материалам пресс-релиза компании Cisco Systems www.mis.ru
9. Исмоилов О.М. “Обеспечение информационной безопасности государственных органов Республики Узбекистан в телекоммуникационных сетях на современном этапе“ Диссертация на соискание степени магистра политических наук ВШСАП РУ, Ташкент, - 2010 г С. - 14
10. Деннинг Д. «Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику» («Activity, Hactivity and Cyberterrorism: The Internet as a Means of Influence on Foreign Policy»). Владивостокский центр исследования организованной преступности, перевод Т.Л. Тропиной http://www.crime.vl.ru/index.php?p=1114&more=1&c=1&tb=1&pb=1
11. Андреев А., Давыдович С. «Об информационном противоборстве в ходе вооруженного конфликта в Косово», Центр практической психологии «ПСИ-ФАКТОР» http://www.psyfactor.org/warkosovo.htm