INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 3, Issue 2, Feb., 2022

CYBER SECURITY: THE CHALLENGE FOR SMALL COUNTRIES

Zaza Tsotniashvili
Professor of Caucasus International University

Abstract

The use of new technologies is becoming increasingly relevant, the development of which is vital for small countries like Georgia.

Cyber security and related technologies have become an important springboard for state security. In the context of the development of information technologies, human weapons are becoming more and more relevant.

There have been many cases in recent years where the significant infrastructure of different countries and companies has been deliberately damaged.

Georgia has experienced significant cyber-attacks on public and private systems, which have caused significant damage to our society. Thus, we consider it important to cooperate with the international community in this direction and increase defense capabilities with appropriate technologies and training of human resources.

Keywords: Information Warfare, Cyber Security, New Technologies, Modern Conflicts.

Introduction

The development of new technologies has led to the creation of new technologies of war in the modern world. The weapon of mass destruction was equaled by the weapon of information. Its actions harm the mental health of people. It damages human consciousness, disrupts the ways and forms of personality identification, and also transforms the memory of the individual. The goal is to influence the opponent's knowledge and perceptions through manipulation.

Information is an important asset and a resource of strategic importance for institutions or states. However, information is nothing in itself if you do not have the tools and infrastructure to disseminate it.

On the other hand, the information conflict is produced by the media. Secondly, it attacks the information technology infrastructure. This refers to attacks on the media via the Internet. Conventionally, such an Internet war is also called a

ISSN: 2776-0987 Volume 3, Issue 2, Feb., 2022

"cyberwarwar," which can be easily distinguished from an information propaganda war. Georgia also had a difficult experience (2008-2020).

The Main Part

Cyber security and related technologies have become an important springboard for state security. "Human weapons (information, psychotropic, economic, etc.) are becoming more relevant in the conditions of information technology development. Technologies for the production of information weapons and information warfare have a special place." (1)

Conducting hostilities in cyberspace as well as on the Internet requires far fewer resources than a conventional attack or propaganda attack.

Cyber-attacks do not require the mobilization of heavy military equipment or the creation of a propaganda strategy and its long-term implementation. It is produced by "hackers" with a simple tactic: a network with thousands of infected computers (i.e., botnets) launches a simultaneous attack on any server.

The attack occurs by sending sequential packets of information to restart and shut down the server: a DDOS attack. Viruses, called Trojan horses (Trojans), are the most common means of infecting computers. The main function of this virus is to penetrate the opponent's system and allow the virus owner to control the target computers.

A botnet is a group of computers managed by one or more people. The botnet is mostly managed by IRC (Internet Relay Chat), but it can also be managed from the site.

One bot is required to control the botnet. Even the creator of the botnet can be chosen as a bot by itself. There are many bots. Everyone has different functions; the botnet creator chooses the bot that has more functions and is easier to manage. In order for a botnet to be more powerful, it needs to have a bot spread. The more widespread and more computers are zombies, the more powerful the botnet is.

There are many things that can be done through a botnet, such as shutting down the Internet, shutting down a server, burning a network card, and more. For this purpose, DDoS (Distributed Denial of Service) is used. Most botnets carry out DDoS attacks. Bots are mostly written in C ++ and C. In order for the bot to spread, it needs to be compiled using Microsoft Visual C++ or LCC-Win 32.

INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 3, Issue 2, Feb., 2022

Trojan horse - Malware, has the ability to perform the desired function and facilitate access to user data. Penetration into other files like a virus is not its purpose. Trojan horses can steal information or damage a computer system. Trojans can use drive downloads or install themselves through online games or online applications to reach the desired computer.

Types of Trojans: Trojan-Spy is a Trojan spy that secretly installs programs such as keyloggers onto a user's computer, allowing a third party to read information typed on the keyboard; Trojan-PSW-steals passwords, and other important information. It can also install other malicious programs. Trojan-Downloader: - secretly writes malicious files to the remote server via the Internet and then automatically installs them on the user's computer;

Trojan-Dropper - contains one or more malicious programs that it secretly installs and uses on a user's computer; Trojan-Proxy - allows unauthorized persons to use the Internet anonymously through the computer; Trojan-Dialer - connects a user's computer to an Internet network via a telephone line. It can also redirect users to unwanted websites.

DOS-attack A denial-of-service attack (DoS attack) A Denial-of-service (DoS) attack is a cyber-attack in which an attacker tries to make a computer or network resource inaccessible to potential users by damaging the connection to the "hosting" for a period of time. Non-use for network and computer consumption is achieved by artificially generating demand for information; a large-scale increase in actual operations hinders and ultimately halts. Such an attack is similar to blocking the exit of a large group of people at the entrance to a store when a legitimate customer no longer has the opportunity to enter, make a purchase, and exit.

It is important to present the information struggle methodology as a tendency to develop socio-political influence, as well as to characterize the methods of dissemination of information desired for the development of the service of modern ideologies. relationship between information warfare production and legal issues. The starting point is again Clausewitz's famous formula: "War is an act of violence, to force the enemy to act according to your will" [2]

In order to understand the issue in more detail, we would like to describe examples of well-known cyber-attacks. The use of computer systems and the Internet has a special place in the work of many countries and organizations.

ISSN: 2776-0987 Volume 3, Issue 2, Feb., 2022

Delaying their work or any kind of damage seriously affects any process carried out by the organization, company, or government agency. The Internet and computer systems are used to manage various infrastructures. "Information has become a high-risk weapon. It is cheap and universal, has unlimited coverage, travels uncontrollably, and often crosses state borders without a low-quality, lie-based permit. "[3]

Damage to any of the military and satellite systems, communications channels, water, gas, electricity, nuclear energy, oil, and refining infrastructure elements can cause serious damage to both the company and the state. Between 2007-2012, there were many cases when the Internet and computer viruses were significantly damaged by the significant infrastructure of different countries and companies.

There are already many examples of cyberom in the world. In our nearest neighbors, the first most famous and high-profile war took place in 2007, between Russia and Estonia. The cause of the cyber-attacks was an initiative of the Estonian people and government.

Russia's confrontation with Estonia escalated into a serious cyber-attack, which created serious problems for the Estonian internet space. Estonian internet resources were inaccessible for some time, Estonian websites were damaged.

Second, we became participants in no less than a large-scale war. No less important, but deadly information war was taking place against the background of the 2008 ground and air military operations between Georgia and Russia. Cameras, newspapers, websites, even cell phones were involved in this war. Both sides tried to provide information to the world only at a convenient time, launching a massive attack on Georgian websites - both government and news and public websites). A large number of network packets were sent to the Georgian Internet space, which led to the congestion of Internet channels and temporary damage to the Georgian Internet space. The main attacks took place on the websites of the Parliament of Georgia and the Ministry of Foreign Affairs, as well as on the websites of news agencies, including one of the Azerbaijani websites (day.az). As a result of the total attack, several sites were shut down (including Media.ge) and government agencies even launched spare blogs - http://georgiamfa.blogspot.com and http://stateminister.blogspot.com/ A rather significant attack was carried out.

INNOVATIVE TECHNOLOGICA
METHODICAL RESEARCH JOURNAL
ISSN: 2776-0987 Volume 3, Issue 2, Feb., 2022

In August 2009, on the anniversary of the Georgian-Russian war "cyxymu", a Georgian blogger and author of a popular and interesting blog, became the target of cyber-attacks. The wave of these cyber-attacks was so powerful that it even shut down foreign networks like Twitter and Facebook. According to unconfirmed reports, the source of all these attacks is Russia - hacker groups or Russian organizations such as RBN - Russian Business Network. After a 10-month investigation in 2009, it was found that there was a network of 1,295 computers in 103 countries. Most of them were located in foreign ministries and agencies, embassies, international organizations, news agencies, and non-governmental organizations. Documents of political, economic, and secret content were extracted and copied from the computers of many diplomats, military representatives, assistant ministers, journalists, and government officials.

Another example is the case of the GeorBot. - In 2011-2012, only those pages of Georgian news sites were hacked by hackers, which contained information about the visits of the NATO delegation, military news, statements by the President, and relations with the United States. Thus, the target audience was pre-selected by the cyber-attack organizers. When opening these websites, the Internet user's computer was automatically infected with an unknown virus program. The virus checked the geographical location of the computer according to the time zone. Many government agencies and several critical infrastructure facilities were infected.

Flame / Gauss - In 2012, a high-level cyber-attack on Arab states was detected. Specially created computer viruses infected the agencies of the target countries. At a later stage, the virus files searched the computer systems and stole sensitive, confidential information (documents, emails, etc.). The virus had the ability to perform video and audio recordings using computer devices. This virus uses encrypted channels of communication.

Stuxnet - is a cyber-attack against Iran's nuclear program. There are various "ICS - industrial control systems." Using the vulnerability found in one such system, the Stuxnet virus was able to intercept the operation of the centrifuges of nuclear reactors and transmit incorrect settings, as well as damage them. As it turned out later, the virus was executed at a highly professional level.

ISSN: 2776-0987 Volume 3, Issue 2, Feb., 2022

Acad / Medre - 2011-2012. The main function of the virus during the cyber-attack was to capture architectural projects from South American states. Its action is revealed only if it finds on the infected computer files, drawings, and projects of the CAD architecture program of interest to the creators of the virus. The retrieved files were transmitted to the authors of the virus on collection servers located in different countries (later infected countries were added to the USA, China, Taiwan, and Spain). From 2007 to 2012, Operation Shady RAT - Cyber Penetration targets more than 70 global companies, organizations, and various structures in several countries.

Conclusion

The main purpose of a cyber-attack is to steal and copy various types of information from an infected agency by all possible mechanisms and technical means. The virus file has the following functions: to send detailed computer information to the author of the virus, to search and copy documents encrypted by the NATO encryption standard, to infect and retrieve information from computers and tablets connected to a computer, high-level encrypted, and hidden virus discovery (control source). According to Kaspersky, the cyber attack allegedly used viral elements created by Russian and Chinese hackers at different times.

High Roller - The target of a cyber-attack is mass global financial manipulations, machinations. Banknote passwords, credit numbers, and transfers are being monitored on the computers of Internet users infected with viruses created by Zeus / SpyEye. Accordingly, the authors of the virus have collected confidential banking information from tens of thousands of users. Some transactions amounted to $ 130,000. The main target is the European states. According to the conclusion of the company McAfee and several financial organizations, cyber criminals managed to carry out illegal transactions of 60 million euros from the accounts of more than 60 financial institutions. According to the report, if the machinations and transactions carried out by all infected computers were successfully completed, cybercriminals would pocket $ 2 billion.

Shamoon - Infecting the computer network of the state oil company ARAMCO, Saudi Arabia. Many of the company's computer operating systems were damaged and temporarily shut down.

ISSN: 2776-0987 Volume 3, Issue 2, Feb., 2022

It took serious human resources and time for the company to fully recover from the work, which caused some damage to the world's richest oil company.

CREECH USB - Infecting the computers of American unmanned aerial vehicle operators via USB devices. The main function of the virus is to steal and transmit aircraft control codes during the mission in Afghanistan. Thus, the use of new technologies in the process of information warfare is becoming more and more important, the development of which is vital for our country. Cyber security and related technologies have become an important springboard for state security. In the conditions of the development of information technologies, human weapons are becoming more and more relevant.

Information is an important resource and one of strategic importance for institutions or states. However, information in itself is nothing if you do not have the tools and infrastructure to disseminate it. There have been numerous recent cases of deliberately damaging important infrastructure in different countries and companies using the Internet and computer viruses. There are already many examples of cyber conflicts in the world. In our neighborhood, the first famous and high-profile war took place in 2007 between Russia and Estonia.

Georgia has experienced significant cyber-attacks on public and private systems, which have caused significant damage to our society. Thus, we consider it important to cooperate with the international community in this direction and increase defense capabilities with appropriate technologies and training of human resources.

References

1. Shonia Supatashvili M. (2009), State Security System, Georgian Technical University. AUTOMATED CONTROL SYSTEMS - No 2 (7).
2. Clausewitz, Karl (1832), On War.
3. Khidasheli T., (2017), From World War II to Cyberwar: How to Win the Information War? https://www.gfsis.org/files/library/opinion-papers/76-expert-opinion-geo.pdf