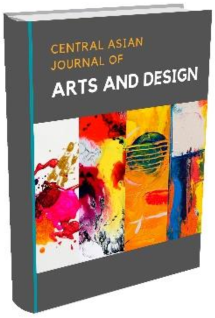
CENTRAL ASIAN JOURNAL OF ARTS AND DESIGN
VOLUME: 3 ISSUE: 1 | 2022

Available online at www.cajad.centralasianstudies.org
CENTRAL ASIAN JOURNAL OF ARTS AND DESIGN
Journal homepage: http://cajad.centralasianstudies.org/index.php/CAJAD



Information Warfare Carried out with Modern Technologies

Zaza Tsotniashvili
Professor at Caucasus International University

Annotation

The development of new technologies in the modern world has consequently led to the creation of new technologies of war. The information weapon equaled the weapon of mass destruction. Its action harms the mental health of people. Before the introduction of viruses into the computer network and the destruction of information. It damages human consciousness, disrupts the ways and forms of personality identification, transforms the memory of the individual. Disrupts stateand armed forces management systems.

ARTICLE INFO

Article history:
Received 01 Nov 2021
Received in revised form 27 Nov
Accepted 29 Dec 2021
Available online 11 Jan 2021

Keywords: Technologies, Warfare, computer network, viruses.

The goal is to influence the opponent's knowledge and perceptions through manipulation. Information is an important resource and resource of strategic importance for institutions or states. He who possesses information also possesses power. However, information in itself is nothing if you do not have the tools and infrastructure to disseminate it. Information conflict is, on the one hand, propaganda produced by the media and, on the other hand, attacks on information technology infrastructure. This refers to attacks on the media via the Internet. Conventionally, such an Internet is also called a cybercomb to easily distinguish it from an information propaganda war. Georgia also has such a difficult experience (2008-2020). Cyber security and related technologies have become an important springboard for state security. In the conditions of development of information technologies, human weapons (information, psychotropic, economic ...) are becoming more and more relevant. "Technologies for the production of information weapons and information warfare have a special place." (1) In cyberspace, conducting the same warfare 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 the so-called "Hackers" with simple tactics: from tens of thousands of infected computers.An established network (called a botnet) launches a simultaneous attack on any server. The attack is carried out by sending sequential packets of information to restart and shut down the server: DDOS-attack. The most common means of infecting computers are viruses called Trojan horses (Trojans). The main function of this virus is to penetrate the enemy's system and allow the virus owner to control the target computers. A botnet is a group of computers run 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 itself can choose a bot. There are many bots and everyone has different functions, the botnet creator chooses the bot that has more functions and which is easier to manage. In order for a botnet to be more powerful it is necessary to distribute the bot, the more common it is and the more computers are zombie the more powerful the botnet is. Many things are possible through Botnet, for example: shutting down the Internet, shutting down the server, burning the network card, and more. DDoS (Distributed Denial of Services) is used for this purpose. Most botnets are set up to launch 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. Trojan horse (Malware Trojan horse) - Malware, which has the ability to perform the desired function and simplify access to user computer data. Its purpose is not to penetrate other files like a virus. 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 - A Trojan spy that secretly installs programs such as key loggers into a user's computer to allow 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 user's computer; Trojan-Dialer - connects a user's computer to an Internet network via a telephone line. It can also redirect users to unwanted websites. Demonstrate important information battle methodology as trends in the development of socio-political influence. Demonstrate the peculiarities of information confrontation methodology. Characterize the methods of disseminating the desired information 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 gain a deeper understanding of the issue, we would like to describe examples of known cyber-attacks.

The use of computer systems and the Internet has a special place in the work of many countries and organizations, therefore the interruption of their work or any kind of damage seriously affects any process carried out by the organization, company or government agency. 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, often of poor quality and based on lies, crosses state borders without permission, and is accessible to all. Military and satellite systems, communication channels, elements of water, gas, electricity and nuclear energy, oil extraction and refining infrastructure. Damage or malfunction of any of them can cause serious damage to both the company and the state. There have been numerous instances where the use of the Internet and computer viruses has deliberately damaged important infrastructure in different countries and companies. There are already many examples of cybermob in the world. In our nearest neighborhood, the first most famous and high-profile war took place in 2007, between Russia and Estonia. The cause of the cyber-attacks was the initiative of the Estonian people and government to relocate a World War II Soviet monument. 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 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, cameras, newspapers, websites, and even cell phones were involved in this war. Both sides tried to provide the world with information that was only favorable to them, and it was at this time that a massive attack was launched 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 attack 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 outIn August 2009, on the anniversary of the Georgian-Russian war. Georgian blogger cyxymu, the author of a popular and interesting blog, became the target of these cyber attacks. The wave of these cyberattacks was so powerful that it even shut down such foreign networks as 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. Ghostnet - Chinese cyber espionage against the Tibetan government. A 2009 10-month investigation found that there were a network of 1,295 computers in 103 countries. Most of them were located in foreign ministries and agencies, embassies, international organizations, news agencies, 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. GeorBot - Targeted cyber espionage against Georgian state resources during 2011-2012. The hackers infected only those pages of Georgian news sites that contained information about the visits of the NATO delegation, military news, the president's statements, 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. The main function - to search for predefined words (military, secret, intelligence) in files and documents in the computer. In case of detection, the mentioned files were copied to the author's server of the virus. Many government agencies and several critical infrastructure facilities were infected. Flame / Gauss - The 2012 high-level cyber attack on Arab states. 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 the appropriate devices on the computer. The virus uses encrypted channels of communication and is difficult to detect due to technical sophistication. Stuxnet - Cyber attack against Iran's nuclear program. There are various infrastructure controls "ICS - Industrial Control Systems". Using a vulnerability found in one such system, the Stuxnet virus was able to intercept the centrifuges of nuclear reactors from an infected system, transmitting incorrect settings and damaging them. As it later turned out the virus was highly professionally executed, spread via USB flash drives, and used still unknown, and undocumented attack methods and vectors to infect systems. 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 Operation Shady RAT - Intensive penetration into more than 70 global companies, organizations and various structures in several countries from 2007-2012 to capture sensitive documentation (financial-economic cyber espionage). Infected agencies: Government agencies of 14 countries, industrial centers, factories (heavy metals, solar energy), electronics-satellite communications (relevant institutions, organizations, factories), military agencies, real estate and financial-banking institutions. infected countries were added to the USA, China, Taiwan, Spain). Night Dragon - Cyber espionage in global oil, energy corporations using viral programs (industrial espionage).

Red October 2007-2012 Large-scale cyber espionage in dozens of different structures of ministries (ministries, embassies, institutions, institutes). The most multifunctional virus among the viruses found to date. The main purpose of the cyber attack - to steal and copy various information from the 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 NATO encryption standard, to infect and retrieve information from computers and tablets connected to a computer, high-level encrypted, and hidden virus Discovery of control source). The cyber attack allegedly used viral elements created by Russian and Chinese hackers at different times (according to Kaspersky).

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 about tens of thousands of users. Some transactions amounted to $ 130,000. The main target is 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 from all infected computers were successfully completed, cybercriminals would cause $ 2 billion. Euro losses. Shamoon - Infecting the computer network of the state oil company ARAMCO, Saudi Arabia. As a result, many operating systems of the company owned by the company were damaged and temporarily ceased to function. It took serious human resources and time for the company to fully resume operations, which caused some damage to the world's richest oil company. CREECH USB - Infecting the computers of American unmanned aerial vehicle operators from USB devices. The main function of the virus is to steal and transmit flight control codes during the mission in Afghanistan. Thus, the use of new technologies in the process of information warfare, the development of which is vital for our country, is becoming more and more urgent.

Cyber security and related technologies have become an important springboard for state security. In the conditions of development of information technologies, human weapons are becoming more and more relevant Information is an important resource and resource of strategic importance for institutions or states. He who possesses information also possesses power. 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 cyberom in the world. In our nearest neighborhood, the first most 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. used literature:

Shonia O., Supatashvili M. (2009), State Security System, Georgian Technical University. AUTOMATED CONTROL SYSTEMS - No 2 (7);

Clausewitz Karl (1832), On War;

Khidasheli T., (2017), From World War II to Cyberoma

How to win the information war? https://www.gfsis.org/files/library/opinion-papers/76-expert-opinion-geo.pdf

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 development of information technologies, human weapons are becoming more and more relevant. Information is an important resource and resource of strategic importance for institutions or states. He who possesses information also possesses power. 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 cyberom in the world. In our nearest neighborhood, the first most 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.