ISSN 2717-7076

IJORCES

INTERNATIONAL JOURNAL OF CONFERENCE SERIES ON EDUCATION AND SOCIAL SCIENCES.

PUBLISHER: ÇORUM: OCERINT -INTERNATIONAL ORGANIZATION CENTER OF ACADEMIC RESEARCH

IJORCES

IJORCES

International journal of conference series on education and social sciences. (Online)

October 2022

Science Editor: **Sari Lindblom**
Vice-rector and professor at University of Helsinki

Copyright © 2022
By Çorum: Ocerint -International Organization Center of Academic Research
All rights reserved.
Available at ijorces.org
Published:
Çorum: Ocerint -International Organization Center of Academic Research
ISSN 2717-7076
Bursa
Bursa, Turkey

Editorial Board Members

Prof. **Hakan Mete Dogan.** Tokat Gaziosmanpasha University, Turkey

Prof. **Afsun Sujayev,** Institute of Additive Chemistry of the ANAS, Azerbaijan

Prof. **Nadir Mammadli,** Azerbaijan Architecture and Construction University, Azerbaijan

Prof. **Munevver Sokmen,** Konya Food and Agriculture University, Turkey

Copyright © 2022

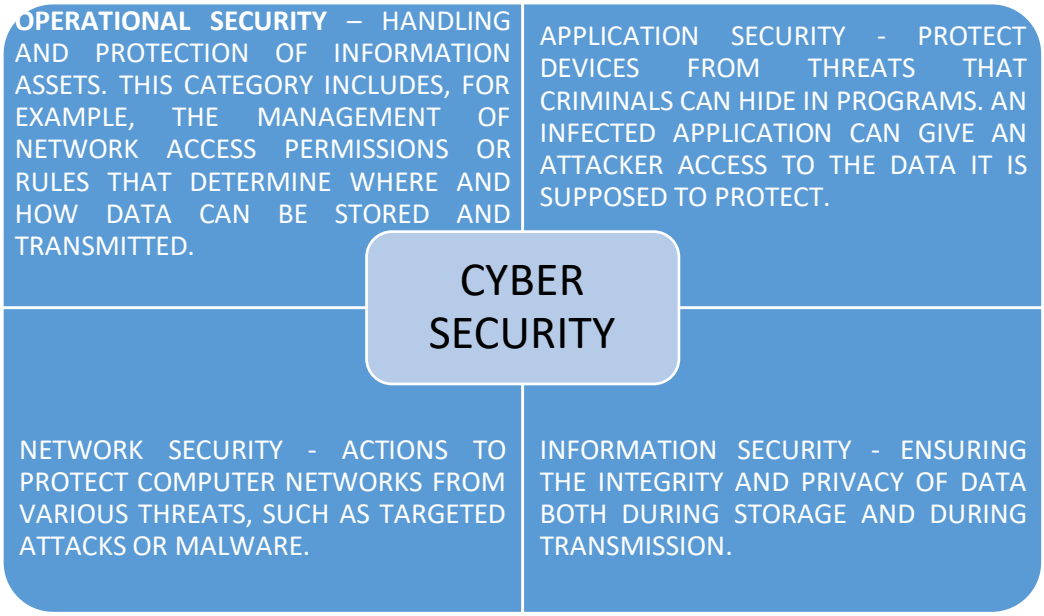
THE MILITARY-POLITICAL CONTENT OF THE CYBER THREAT AND CYBER SECURITY CONCEPTS

Batirov Farkhod Avazovich
University of Public Safety of the Republic of Uzbekistan

Abstract: Cybersecurity (sometimes referred to as computer security) is a set of techniques and practices for protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Cybersecurity finds application in a wide variety of areas, from business to mobile technology. Nowadays, cyber security is increasingly threatened by cyber attacks, crime and privacy disclosure, which are penetrating areas like politics, economy, culture and society. All countries are strengthening their attention to cyber security and have taken a series of actions in accordance with their own situation and the world Internet development to improve their capacity of cyber security assurance. Cyber-attacks are becoming more hidden but more destructive.

Key words: cyber security, cyber-attacks, peacocking, organized attacks, virus, web spoofing, threat, power of destruction.

Even the most secure system can be attacked due to someone's mistake or ignorance. Therefore, every organization should train employees and tell them about the main rules: for example, not to open suspicious email attachments or connect questionable USB devices. There are 4 types of cyber security:



Cybersecurity is one of the most important topics in the modern world today. But first, it is necessary to separate the concepts of cybersecurity and information security, which are confused by a huge number of people. Cybersecurity is primarily a subset of information security.

Information security is another way of saying "data protection". Most companies today store data on servers, desktops, laptops or anywhere on the Internet - but just a decade ago, before all confidential information went online, it filled entire offices. And some confidential information remains there to this day! The main task of information security is the protection and safety of data in any form, and this is a broader meaning than that of cybersecurity. Cybersecurity, on the other hand, is about protecting data that is stored

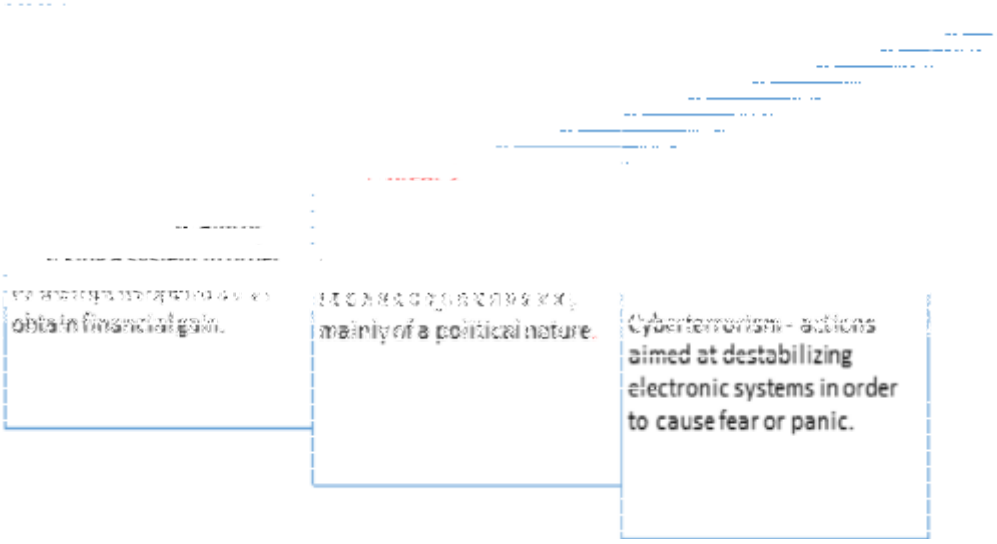
in electronic form. And also in determining the most important data, where they are located, and what technologies should be used to protect them.

We all live in a world that today is connected by networks and information technologies, from Internet banking to government infrastructure, and that is why cybersecurity is a necessity. Concern about cyberattacks today is taking on a global scale, as hacker attacks can, for example, undermine the world economy or cause enormous damage to the image of a country.

In Kazakhstan, the issue of cybersecurity is extremely acute due to the lack of a security standard. This is provided that today this topic cannot be ignored. "According to astudy by Juniper Research, global damage from cyber attacks has quadrupled.While maintaining the current level of cyber attacks, the total losses of the global economy by 2019 will amount to $2.1 trillion." If we take our closest neighbor Russia, then the damage from cybercrime in 2015 amounted to 6 billion rubles [2]. Whereas in Kazakhstan and in many other countries of the world, such data is not disclosed or even considered.

As example, we will give the recent information about cyber attacks: in February 2016, a hacker attack was carried out on the central bank of Bangladesh, during which losses amounted to $81 million and an attempted theft of another $850 million was prevented. At the beginning of August 2016, the data of 200 million Yahoo user accounts were put up for sale online. This data includes usernames, passwords, and dates of birth. Every year, about 500 million host computers are attacked by botnets, 18 computers per second. Technically peacocking represented by CIH virus and Code Red virus are replaced by purposeful and organized attacks. Governmental intervention is being deepened: web spoofing, DDoS, Trojan and botnet, and cybercrime are the major threats to cyber security. In 2016, at least 255,100 phishing attacks happened worldwide, an increase of over 10% in comparison with the number in 2015. Actually, the number in 2021 was unprecedentedly high. Advanced persistent threats are becoming increasingly serious with great power of destruction, imperceptibility, durability and complexity, posing great threat to critical infrastructure of finance, business, communication and transportation, and national defense. "The number of ransom software attacks is growing explosively. By the end of 2016, such software had evolved into a family-like development mode, with 44,300 new varieties having been discovered and 114 countries having been affected. RaaS is developed into a black industrial chain. From 2016 to 2021, the market scale of the underground market of ransom software saw an increase of 2502%." Large-scale data breach happens frequently, threatening the security of data from governments, businesses and individuals. From 2008 to 2016, over seven billion pieces of online ID information worldwide was embezzled, which indicates that every person's information is embezzled once.The governmental dataof Sweden, Mexico and the Philippines were disclosed, which should arouse the attention of all governmental sectors. With the maturity of IoT and AI, the equipment of IoT and AI may be the major targets of cyber attacks. "By the end of 2016, it had been discovered that 2526 control servers had controlled 1.254 million intelligent devices of IoT of the world." Therefore, we should attach equal importance to security and development and take actions in advance to prevent any attack. The United States, Russia, China, Germany and Singapore have launched national cyber security strategies and established special organizations to strengthen the protection of critical infrastructure. They also enhance cyber content security supervision and promote the development of cyber security industries. The position of cyber security has been elevated in the overall national security. Some countries have channeled cyber security into military security to enhance its importance. Some foreign organizations attract attackers for a good reason - financial and medical data can be stolen from them. However, any company can become a target, because

criminals can hunt for customer data, spy on or prepare an attack on one of the customers. International Data Corporation predicts that if the number of cyber threats continues to grow, spending on cyber security solutions will reach $133.7 billion by 2022.



Spyware is software that secretly monitors user activity and collects information (such as credit card information). Then cybercriminals can use it for their own purposes. Ransomware encrypts files and data. The criminals then demand a ransom for the restoration, claiming that otherwise the user will lose the data. Adware - advertising programs that can distribute malware. Botnets are networks of computers infected with malware that cybercriminals use for their own purposes. SQL injection- this type of cyber attack is used to steal information from databases. Cybercriminals exploit vulnerabilities in data-driven applications to spread malicious code in the database management language (SQL).

Fishing	is an attack that aims to trick the user into obtaining confidential information (for example, bank card details or passwords). Often in these attacks, the perpetrators send emails to the victims, pretending to be an official organization.
Man-in-the-Middle attacks ("man in the middle")	is an attack in which a cybercriminal intercepts data during its transmission - it becomes, as it were, an intermediate link in the chain, and the victims are not even aware of it. You can be exposed to such an attack if, for example, you connect to an unsecured Wi-Fi network.
DoS attacks (denial of service attacks)	Cybercriminals create excessive load on the networks and servers of the target of attack, due to which the system stops working normally and becomes unusable. For example, attackers can damage critical infrastructure components and sabotage an organization's operations.
Dridex Troyan	a banking Troyan with a wide range of capabilities that appeared in 2014. It infiltrates victims' computers using phishing emails and malware. Dridex can steal passwords, bankcard details and personal information of users, which are then used by scammers. The amount of financial damage caused by them isestimated in hundreds of millions. In December 2019, the US Department of Justice accused the leader of a group of cybercriminals of participating in an attack using the Dridex malware. This campaign has affected public, government and business structures around the world.

In order to protect yourself, Cyber Security Center recommends keeping your devices up to date with the latest security patches and antivirus software, and backing up your files regularly.

Used literature.

1.Babash, A.V. Information security: Laboratory workshop / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2019. - p. 54-59

2.Baranova E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - p. 104-111

3. Biryukov, A.A. Information security: protection and attack / A.A. Biryukov. - M.: DMK Press, 2013. - p. 154-156

4. Gafner, V.V. Information Security: Textbook / V.V. Gafner. - Rn / D: Phoenix, 2010. - p. 254-260

5.Glinskaya E.V. Information security of computer structures and systems: Textbook / E.V. Glinskaya, N.V. Chichvarin. - M.: Infra-M, 2018. - p. 94-97.

6.Grishina, N.V. Information security of the enterprise: Study guide / N.V. Grishin. - M.: Forum, 2017. - p. 164-169.

7.Zapechinkov S.V. Information security of open systems in 2 volumes v.2 / S.V. - M.: GLT, 2008. - p. 37-41.

8.Konotopov, M.V. Information Security. Laboratory workshop / M.V. - M.: KnoRus, 2013. - p. 107-110.

9.Kuznetsova A.V. Artificial intelligence and information security of society / A.V. Kuznetsova, S.I. Samygin, M.V. Radionov. - M.: Rusajns, 2017. - p. 64-69.

10.Malyuk, A.A. Information security: conceptual and methodological foundations of information protection - M.: GLT, 2004. - p. 280-283.

ELSEVIER SSRN Universal Impact Factor