Cyber Defense Is A Modern Component Of Ukraine's Security

Oleksandr Lavrut [1], Tetiana Lavrut [2], Vladyslav Kolesnyk [3], Halyna Kolesnyk [4], Serhii Bohutskyi [5] and Leonid Polishchuk [6]

[1,2,3,5,6] *Hetman Petro Sahaidachnyi National Army Academy, 32 Heroes of Maidan street, Lviv, 79026, Ukraine*
[4] *Lviv Polytechnic National University, 12 Bandera street, Lviv, 79013, Ukraine*

Abstract

The report is devoted to the topical issues of cybersecurity in modern society. It is shown that with the beginning of the war in eastern Ukraine, both the population and infrastructure of Ukraine are significantly affected by cyber attacks. The examples of ways to solve cybersecurity issues in the civil society as well as in the security apparatus of Ukraine that have already been implemented are given. The authors also consider the prospects for the development of this area.

Keywords

cyber security, cyber defense, cyber threat, cyberspace, cyber attack

1. Introduction

In the era of globalization, information technology and telecommunication systems occupy all spheres of human life and the state activity. The volumes of information are growing, technical means are changing, and, accordingly, the risks of information security in information and telecommunication systems are growing both in the civil society and in the security apparatus [7, 9]. Security depends on the use of available opportunities and the proper reaction to emerging threats in cyberspace. Essential infrastructure, national defense and the daily lives of citizens depend on computer and interconnected information technologies. All spheres of life have become more dependent on secure cyberspace; new vulnerabilities are identified and the number of new threats grows.

Cyberspace, along with land, air, sea, and space, is recognized as a new operational space, and cyberspace is an integral part of the hybrid war. Leading countries of the world such as the United States, Great Britain, China and others pay the most attention to operations in cyberspace.

Therefore, the issue of security in cyberspace has always been urgent in the world. Today, the consequences and effectiveness of cyber weapons can be equated to weapons of mass destruction.

2. Measures to ensure cyber protection in the state

Since the beginning of the confrontation with Russia, cyberspace has become another platform for military action. The experience shows that the population and infrastructure of any state are really affected by cyber attacks Today, everyone is a subject of cyberspace. The laptop, tablet, mobile phone are potentially vulnerable gadgets. The simplest threat that anyone in the world can face is sending links and phishing emails with incomprehensible suggestions. Such emails can download malicious software, block your phone

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine
EMAIL: alexandrlavrut@gmail.com (A. 1); lavrut_t_v@i.ua (A. 2); vector-ua@ukr.net (A. 3); galyna.o.kolesnyk@gmail.com (A. 4); sergij-b@ukr.net (A. 5); vl.kolesnyk@ukr.net (A. 6)
ORCID: 0000-0002-4909-6723 (A. 1); 0000-0002-1552-9930 (A. 2); 0000-0001-5257-3124 (A. 3); 0000-0003-1912-1649 (A. 4); 0000-0001-7454-8894 (A. 5); 0000-0002-4379-3990 (A. 6)

or computer, break into your system, extort money, use your personal information, and more. That is why cyber defense reform has begun in Ukraine [6].

The National Cyber Security System of Ukraine is a set of subjects of cyber security and interconnected measures of political, scientific and technical, informational, educational nature, organizational, legal, operational and investigative, intelligence, counterintelligence, defense, engineering and technical measures, as well as measures of cryptographic and technical protection of national information resources, cyber protection of critical information infrastructure [4].

Our state has to to react quickly to new threats and search for effective cyber defense measures. The issue of cyber defense in the country can be solved only through a comprehensive approach. Some decisive steps have already been taken in this direction at the state level. Thus, during the All-Ukrainian Forum "Ukraine 30. Country Security" the Cyber Security Center was opened. The center is a structural subdivision of the State Service for Special Communications. The institution will be oriented as a service structure that will provide cybersecurity services, ranging from individuals to public authorities. One of the heads of the State Service for Special Communications and Information Protection of Ukraine, Deputy Head of the State Special Communications Service Oleksandr Potiy presented the Organizational and Technical Model of cyber defense during his speech at the scientific-practical conference "Information and Telecommunication Systems and Technologies and Cyber Security: New Challenges, New Tasks" [2, 8]. He explained that if we consider cybersecurity as a targeted activity to ensure the security of cyberspace, it is necessary to determine the structure of such activities, the subjects of cybersecurity, the goals of cybersecurity and the appropriate infrastructure that will support these activities [2, 8]. Organizational and technical model of cyber defense will consist of three vertically and horizontally integrated infrastructures (Fig.1)

The first level is the organizational and managing infrastructure of cyber defense. The components of this infrastructure are the subjects of the national cybersecurity system, which are defined by the relevant legislation at present. Cybersecurity entities are grouped into the public, academic, private, public and regional sectors.

The second level is the technological level or technological infrastructure of cyber defense, which consists of a set of forces and means of cyber defense. These are the relevant technology units of cybersecurity subjects in various sectors. At this level, the appropriate interaction of technological units is provided, i.e information exchange, monitoring, ensuring the sustainable security of cyberspace. The technological infrastructure has three horizons - national, sectoral (regional) and object.

The third level is the basic cybersecurity infrastructure, which provides the fundamental capabilities of cybersecurity. The basic infrastructure consists of two layers: a protected information infrastructure and a knowledgeable society (communities and citizens).

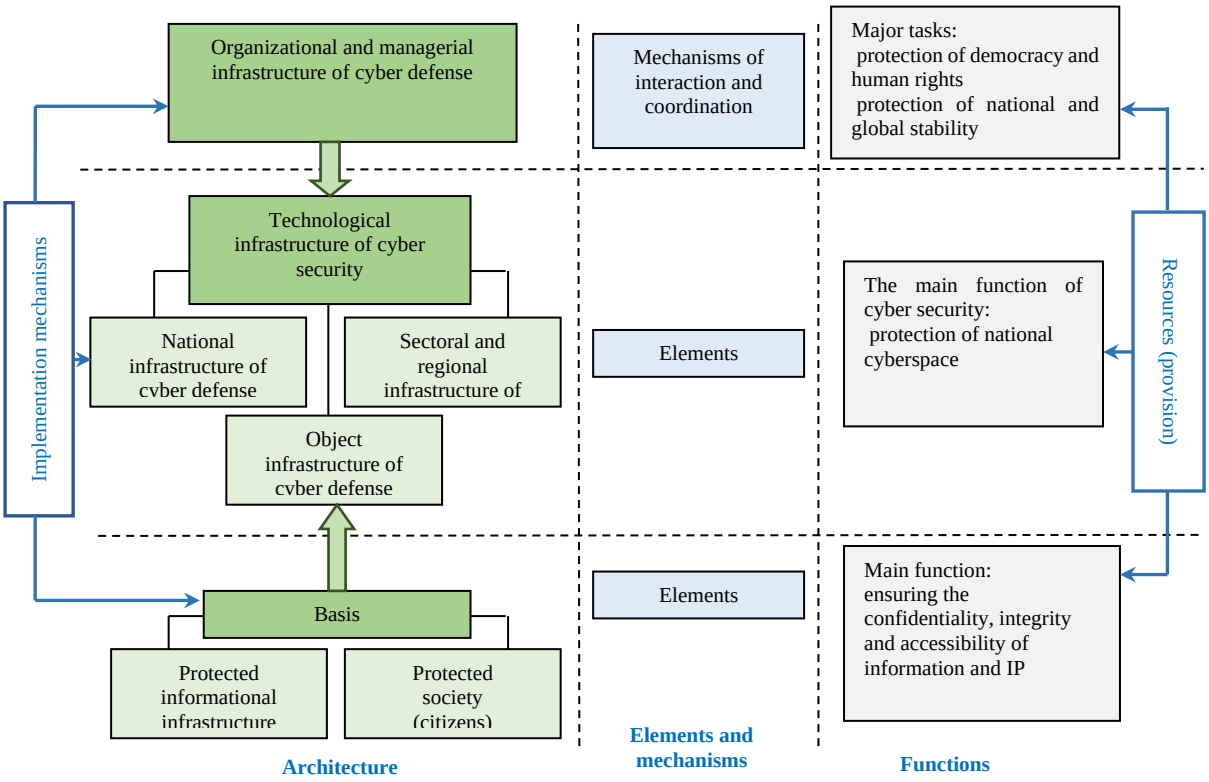

Figure 1: Organizational and managerial infrastructure of cyber defense

Let us consider baseline cybersecurity threats. They can be classified as follows:

1) **Threats from authorized users.** This includes intentional or unintentional (as a result of negligence) actions of employees working with the information system. Such actions may result in theft, destruction or alteration of data on servers or workstations without any third-party interference with the information infrastructure.

2) **External targeted external attacks.** This group includes actions that involve unauthorized intrusion into a computer network from the outside, as well as DDOS attacks. The purpose of such attacks is often to destroy or steal confidential information, change the algorithms of networks and equipment, delete server data, interfere with management systems. DDOS attacks aim to cause congestion on communication channels, servers or nodes of networks, which leads to loss of functionality or a sharp decrease in the performance of these systems.

3) **Computer viruses.** This group is the most dangerous for the information infrastructure, as it is the most common. The source of virus penetration can be e-mail, the Internet, external media, etc. The virus can result in both the theft of information (usually access passwords) and its destruction.

4) ***SPAM*** is a message (mass mailing) coming from unauthorized sources. Today, spam has become so widespread that it can be definitely attributed to sources of information security threats. A lot of spam comes to users' email addresses being the main method of remote virus transmission and can be a source of infection for workstations or simply overload mail servers or routers.

5) **Force majeure** may be refered to a separate group. These include damage to equipment due to wear, misuse or external factors. Such circumstances can also lead to data loss, and they must also be taken into account in the process of designing an information security system.

Today, there are many ways to deal with information security threats. For each threat, its own methods and processes are selected, which control certain "nodes" of the information system and prevent any failures in their work. However, the maximum effect can be achieved only by applying all these methods in combination. That is, the design, construction, implementation and maintenance of information security is a complex task that requires the analysis of potential threats, the choice of methods to combat them and establish interaction between these methods.

Basic means and methods of information protection:

1) **Authentication system.** This is the main method of information protection in almost any field. It comes down to the fact that to gain access to a particular information area, management console or communication channel, the user must provide the system with their authentication data (usually a name and password). The system then compares this data with

predefined security policies, and afterwards gives or denies the user access to the requested information. Thus, each user in the information structure has its own personal ID and level of access, which allows him to perform any action only within this level.

2) **Encryption system.** This system is designed so that an attacker who managed to intercept certain data (e-mail, portable storage device ...) could not access with this data without having a specific key. There are many methods of data encryption, but they are all divided into 2 types. They can be distinguished into private key encryption and public key encryption. The former involves the presence of 1 key for encrypting and decrypting data, while the letter involves the presence of 2 different keys and is the most stable method.

3) **Firewall.** The use of a firewall aims to separate the local network from the global Internet. The firewall has its own security policies and access restrictions, so the interaction between the local network and the global one becomes possible only within these policies.

4) **Virtual Private Networks (VPNs).** This technology allows data to be transmitted over global public networks, such as the Internet, through encrypted VPN tunnels. Thus, although the information is transmitted over the global network, it cannot be accessed from it without authorization.

5) **Email filtering.** This system allows setting certain filters on the content of incoming and outgoing correspondence. This protects the internal network from the intrusion of unwanted data, in particular viruses, as well as eliminating the leakage of certain types of information from the internal network.

6) **Control of nodes efficiency.** Control focuses on constant monitoring of serviceability and quality of servers, workstations and network equipment. It helps anticipate and prevent equipment failures that could result in information loss.

7) **Antivirus protection.** It is focused on preventing threats from computer viruses. Closely related to email filtering and firewalls.

8) **Using vulnerability detection systems.** It helps to identify weaknesses in the information security system by modeling the actions of an attacker and testing the system during such actions.

9) **Creating a back-up copy.** The backup system allows backing up certain data.

Information security is one of the main conditions for the normal operation and development of the information system of any enterprise, as well as helps to minimize the possibility of information leakage.

And separately consider the "human" factor, which is the most risky component of this system (Fig. 1). It is human ignorance, negligence and mistakes that lead to such violations as:

- insufficient users awareness of the basics of information protection and misunderstanding of the need for their careful observance;
- the use of uncertificated or uncertified technical means of processing classified data, because this equipment, at best, may simply be just crude, and at worst - it may contain inserts at the physical or software levels;
- poor control over the observance of information protection rules by full-time or part-time information security and cyber security services and engineering units that do not properly monitor the serviceability of equipment or lines;
- staff turnover, because they have information with limited access or official data.

All these factors do much more harm than a whole group of attackers [5].

And so it becomes clear that the mechanisms of implementation of the model (Fig. 1) and its resource provision are the most important components that cover all levels of architecture. Development and improvement of the regulatory framework through the adoption of relevant legislation, regulations, standards, orders at all levels will further allow to implement this model.

3. Measures to build the transport platform of the national telecommunication network

Within the framework of creation of the protected infrastructure of the state and performance of tasks concerning creation and maintenance of functioning of the National telecommunication network actions on construction of a transport platform of the National telecommunication network, system of operational and technical management and automation of activation of services are carried out. In order to create a transport platform of the National Telecommunication Network (hereinafter TP NTM), the following steps have been performed today.

The construction of the first and second stages of the optical segment of the NTM transport platform has been completed. In this area of work, in particular, a system of operational and technical management and automation of activation of NTM TP services has been developed. As part of the construction of the third stage, the development of project documentation of the "Project" stage was provided, which received a positive expert opinion; After obtaining a construction permit, the deployment of telecommunication nodes will be launched at the technological sites of state bodies, which will enable even more state bodies to receive NTM services.

In order to increase the reliability of NTM operation at the interregional level and create opportunities for providing NTM services in the field to stationary, mobile, including mobile facilities, design work on the object "Construction of the satellite segment of the transport platform of the National Telecommunication Network" was provided. In order to create a radio segment of the NTM transport platform, the operation of two research areas is ensured, the results of which are included in the technical requirements for the creation of this segment. To ensure the functioning of the state management system in emergency situations and during special periods, the State Service for Special Communications and Information Protection of Ukraine has started design work on the object "Construction of the mobilization segment of the transport platform of the National Telecommunication Network".

Based on the result of the design, the best option will be taken to create a mobilization segment of the transport platform of the National Telecommunication Networks, which will ensure reliable operation of the state management system, as well as obtaining the necessary modern unified communications services directly at secure control points.

Today, in order to develop a technological platform for the deployment of the national cyber resilience system, measures are being taken to develop an organizational and technical model of cyber security as a set of systems, complexes and measures designed to ensure cyber security of critical infrastructure and cyber security of state electronic information resources and its telecommunications platform - National Telecommunication Network.

The implementation of the organizational and technical model of cyber security as a component of the national cyber security system is carried out by the State Center for Cyber Defense, which ensures the creation and operation of the main components of the system of secure access to the Internet, antivirus protection of national information resources, vulnerability detection and response to cyber incidents and cyber attacks, systems of interaction of teams responding to computer emergencies, as well as in cooperation with other actors of cyber security develops scenarios for responding to cyber threats, measures to combat such threats, programs and methods of cyber training.

In the context of organizational and technical measures attended to prevent, detect and respond to cyber incidents and cyber attacks and eliminate their consequences, a key element of the organizational model is the Cyber Threat Response Center (CRC).

Also, the State Center for Cyber Defense (Cyber center UA30) has already been established in Ukraine - an institution that directly deals with the protection of state information resources. It provides services not only to government agencies but also to citizens and businesses. In May 2021, with the participation of the President of Ukraine, its official opening took place. The main task of the center is to ensure that the vast majority of state registers are under its protection until 2024.

Cyber center UA30 is part of the State Service for Special Communications and Information Protection of Ukraine. This is the newest state center for responding to cyber incidents, gaining skills and knowledge in the field of cyber security. It also includes an updated training ground with a unique technology for testing real scenarios of cyber attacks in the learning environment. There are only about 20 such platforms in the world, six of which are in the United States [1].

The UA30 cybercenter will have four priorities:

1. Protection of state registers. At this stage, any threats related to database intrusion will be monitored and eliminated. The main goal is to have 100% of the infrastructure sensors that prevent hacker attacks in 3 years. In addition, the creation of a unified Platform for the deployment and maintenance of state registers has already begun. This will allow to create and maintain multi-level registers according to uniform principles and standards that will comply with current legislation.
2. Protection of citizens, private information and business. Citizens of Ukraine will have available tools and adequate knowledge for their own protection. Businesses will be able to protect their information and processes by improving national standards and practices. Private information of citizens will be reliably protected because the Cyber Center provides appropriate response services to cyber threats.
3. Development of cyber hygiene culture. The center will be an educational hub, where everyone will receive knowledge to protect themselves on the Internet. Cyber hygiene is one of the foundations of digital literacy. Currently, 53% of the country's population has a low level of digital skills. This indicator must be changed immediately.
4. Formation of a personnel reserve of cyber security. Today, there is a shortage of cyber security professionals around the world. It is important to change this situation. Therefore, the creation of a network of cyber security training centers is a priority.

The State Center for Cyber Defense is taking measures to counter cyber attacks. Also, owners of information systems, heads of departments responsible for information security of state bodies of Ukraine are constantly provided with recommendations on combating cyber attacks, as well as work conducted to prevent contamination of the infrastructure with malicious software.

In order to ensure effective exchange of information on cyber incidents, analysis of trends, identification of the main sources of cyber incidents, effective counteraction to cyber threats and exchange of risk data, the national Malware Information Sharing Platform

"Ukrainian Advantage" (MISP-UA) has been launched [3]. The use of the system allows cyber specialists of the Security Service of Ukraine to anticipate ways of attacks, potential threats and neutralization tools for further response. In terms of its functional content, the platform allows to strengthen the state of cyber security of various sectors of public administration and the economy of Ukraine. With its help a public-private interaction takes place for joint protection of information and cyberspace of the state as a whole.

Ukraine is currently in the process of joining NATO's Joint Center for Advanced Technology in Cyber Defense, which provides anti-cyber attacks and cyber protection of information systems [10].

4. Conclusions

Ukraine is now at the forefront of the fight against cyber challenges. Digitalization and cyber security always go the same way. Therefore, the field of cyber security should not just be on a par with the digitalization of the country, but one step ahead. However, it is not worth relying only on the fact that all cyber security issues will be resolved by the state. Every person, every citizen should know how to secure and protect themselves, their confidential data, bank accounts, etc.

Thus, the issue of cyber security is certainly relevant. Its solution should be comprehensive both at the level of ordinary users and at the state level in the framework of creating a modern legal framework, appropriate software and technical solutions. Increasing investment in cyber security will help prevent attacks on large public and private companies and counter intentions to destabilize society.

5. References

[1] The UA30 Cybercenter has been opened in Ukraine, which will protect the state from cyber attacks. URL: https://www.kmu.gov.ua/news/v-ukrayini-vidkrili-kibercentr-ua30-yakij-zahishchatime-derzhavu-vid-kiberatak

[2] Organizational and technical model of cyber defense was presented in Ukraine. URL: https://softline.org.ua/news/v-ukraini-prezentovano-orhanizatsiino-tekhnichnu-model-kiberzakhystu.html

[3] To counter cyber threats, the SSU launches an updated version of the MISP-UA platform. URL: https:// ssu.gov.ua/novyny/7800

[4] LAW OF UKRAINE "On Basic Principles of Cyber Security of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/2163-19

[5] Cybersecurity as an important component of the entire state protection system. URL: https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html

[6] Cyber Defense of Ukraine: state, problems and current measures to ensure it. URL: http://opk.com.ua/кібероборона-україни-стан-проблеми-т/

[7] Lavrut O.O. New technologies and means of communication in the Armed Forces of Ukraine: the way of transformation and prospects of development / O.O. Lavrut, T.V. Lavrut, O.K. Klymovych, Ю.M. Zdorenko. Science and technology of the Air Force of the Armed Forces of Ukraine. 2019. Vol. 1 (34). P. 91–101. DOI: 10.30748/nips.2019.34.13.

[8] Oleksandr Potiy, Andriy Semenchenko, Dmytro Dubov, Oleksandr Bakalynsky, Danylo Myalkovsky. Conceptual principles of implementation of organizational and technical model of cyber defense of Ukraine. URL: DOI: https://doi.org/10.18372/2410-7840.23.15434.

[9] Puzyrenko O.H., Ivko S.O., Lavrut O.O. Analysis of the process of information security risk management in ensuring the survivability of information and telecommunications systems. Information processing systems. 2014. Vol. 8 (124). P. 128-134.

[10] The process of including Ukraine in the NATO Cyber Defense Center has begun. URL: https://www.pravda.com.ua/news/2021/06/7/7296338/