# Cyber security in the national security & defence sector of Ukraine: today's challenges and ways to avoid possible threats

Ihor Proshchyn [A]; Volodymyr Shypovskyi [B]

**Received:** January 26, 2020 | Revised: February 28, 2020 | Accepted: February 29, 2020

**DOI:** 10.33445/sds.2020.10.1.1

***Abstract***

Development of strategic communications is necessary for the effective preparation and use of the Armed Forces, for the coordination of actions of state bodies in defence matters, as well as for the purpose of forming and strengthening the confidence of Ukrainian society in the state's military policy. The basic elements of strategic communications of the Ministry of Defence and the Armed Forces are public relations, public relations in the military sphere, public diplomacy, information and psychological operations.

In turn, one of the components of the information operations system is cyberspace actions. The strategic importance of actions in cyberspace is due to the fact that cyber threats today, with devastating consequences, pose no less danger than direct military intervention. In 2016, during the Summit of Heads of State and Government of the North Atlantic Treaty Organization, the first ever EU-NATO security cooperation agreement was signed, in particular on hybrid wars and cyberattacks. Cyberspace, along with land, air, sea, and space, has been recognized as a new operational space, and cyber-operations (cyberattacks) are an integral part of the hybrid war. Also, cyber weapons in terms of scale of successors are compared with weapons of mass destruction. In this regard, cyber security is one of the top priorities for the state.

The article is devoted to the research of actual problems of providing the cyber security of the Armed Forces units of Ukraine in the current conditions of development of the information society and during hybrid threats from the Russian Federation side. The authors explain the basic concepts and definitions of the scientific field and explain conceptual approaches to cybersecurity and propose some ways to improve the existing cybersecurity mechanism or how to enhance it.

***Keywords:*** strategic communications, hybrid warfare, cybersecurity, cyberthreats, information security, critical infrastructure objects.

## Introduction

For the sixth year in a row, Russia has been waging a hybrid war against Ukraine. This type of war implies that the aggressor country may remain publicly implicit in such a conflict and conduct covert military operations. Hybrid war is both the conduct of hostilities under the auspices of illegal (informal) armed groups and the simultaneous use of a wide range of political, economic (energy and trade-economic), as well as advocacy measures, from which this usually launches hybrid warfare and its accompanying throughout the period of hostilities. As you can see, all of the above-mentioned points are now directed against Ukraine.

**Analysis of recent research and publications.** The study of the state of scientific development of cyber security problems of the Armed Forces of Ukraine showed that no special research on these issues was conducted at the present stage. However, some aspects of cybersecurity were considered in the scientific works of V. Chernega, V. Konakh, V. Lipkan, A. Orleans, E. Tikhomirova and others.

[A] National Defence University of Ukraine, Senior instructor of Section of Strategic Communications of the Educational and Research Center of Strategic Communications in the Sphere of National Security and Defence. 28, Vozduhoflotsky, ave, Kyiv, 03049, Ukraine, *e-mail:* pros4in@ukr.net, ORCID: 0000-0001-6686-5603

[B] National Defence University of Ukraine, Senior research officer of Research Section of the Educational and Research Center of Strategic Communications in the Sphere of National Security and Defence. 28, Vozduhoflotsky, ave, Kyiv, 03049, Ukraine, *e-mail:* vladimir.shipovsky@gmail.com, ORCID: 0000-0003-3743-3064

## Material and Method

**The purpose of this article** is the presentation of the result of studies of current problems of ensuring cyber security of the Armed Forces of Ukraine in the current conditions of development of information society and during hybrid threats by the Russian Federation and clarification of the basic concepts and definitions of the scientific direction; definition of conceptual approaches to security in cyberspace and promising ways to improve the existing cybersecurity mechanism, and ways to increase the level.

## Results and discussion

*Cybersecurity* is the protection of vital interests of the individual and the citizen, society and the state in the use of cyberspace, which ensures sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine [1].

*Cyberspace* is an environment (virtual space) that enables communications and/or public relations to be created as a result of the operation of interoperable (connected) communications systems and the provision of electronic communications using the Internet and/or other global data networks [2].

Actions in cyberspace are conducted to:

provision and support of other measures of information operation;

reducing the ability of the enemy to use cyberspace;

destructive effects on hostile information infrastructure and information resources. Actions in cyberspace can be directed to both infrastructure and information processes that take place, and indirectly to human consciousness.

*Forms of actions in cyberspace* carried out in the framework of (in the interests of) an information operation: cyber-attack, cyber-attack, cyber intelligence and cyber defence, or their mutually agreed set – *cyber operation.*

Let's take a closer look at what the effects of the most common types of cyber-attacks can be:

*Vandalism* is an attack that strikes at the authority of the state both in the world and among the population, in simple words, it causes reputational losses. Such cyber-attacks include defamation of official web pages, replacement of content with offensive or propaganda images.

*Propaganda* is a spamming newsletter that contains information about paganism, fake news to promote a profitable perspective and disorientation of the population. If it were not for the propaganda in Crimea, Luhansk and Donetsk oblasts, Russia would not have found support among the local population in 2014. The propaganda began long before the events of 2014, was ongoing and focused on a certain segment of the population, the so-called target audience.

*Information Gathering (Cyber espionage)* – hacking private pages or database servers to gather valuable information and replace it with information that is useful to the other party. For example, misinformation and theft of troop movements in the area of warfare will lead to inevitable casualties.

*Denial-of-service (D-dos)* operations are attacks from a large number of computers, the primary purpose of which is to disrupt the functioning of websites or computer systems. For example, if there is a malfunction and error in the system responsible for processing the data received from the demarcation line, this could result in the commander not being able to make the right decision.

*Interference with hardware* – attacks on computers or servers that, for example, enable the communication of civilian or military systems, which in turn will cause shutdowns or errors in data exchange, and even worse – will lose communication and therefore the ability to manage the operations of the units.

*Attacks on Critical Infrastructure Objects* – Attacks on computers and systems that provide livelihoods for settlements, including water, electricity, transport, and more [3].

With regard to cyber intelligence measures, they are aimed at extracting data in the cyberspace of the enemy, monitoring his automated control systems, information systems and the processes circulating in them, searching for these gaps in the security subsystem.

Leading countries in the world, such as the United States of America, the United Kingdom, China, and others, pay the most attention to cyberspace operations. They have huge investments in the budget for the development of the cybernetic component of the armed forces, as well as constantly implement programs for national security and protection of critical infrastructure against cyberattacks. As no one can say with certainty that its networks are fully secure and capable of resisting multi-vector cyberattacks, cyber security has become a priority in many countries [5].

A number of leading Western experts have falsely called the hybrid war a “new generation war” or a “new generation war”. Its developer is considered to be Valery Gerasimov, Chief of the General Staff of the Armed Forces of the Russian Federation, who in February 2013 in his article “The value of science in foresight” outlined the basic principles of hybrid wars. Subsequently, these principles of conducting “nonlinear” operations were called the “Doctrine of Gerasimov”. And it was the hybrid war against Ukraine that became one of the reasons for the rapid development of cyber security units in the leading countries of the world.

The Russian Federation is constantly increasing its number of cyber espionage operations and is increasingly trying to influence public opinion in our country by using fake news and outright propaganda. The main purpose of these operations is to loosen the situation in the country, create chaos and panic as a basis for promoting their own interests [6].

Russia also conducts cyber operations against critical infrastructure, the private sector, and information and telecommunication systems of the Armed Forces of Ukraine. One of the latest examples of a simple, yet large-scale, private-sector intelligence operation is BugDrop. It focused on gaining remote access to personal computers, laptops, smartphones, tablets and other gadgets of employees of various structures, which resulted in the personal data and passwords of employees of critical infrastructure, media and scientific institutions being abducted and uploaded to Dropbox [8]. The attackers were able to gain access to the computers by sending them phishing emails inviting them to open a Microsoft Word file containing a malicious macro. Thus, at the touch of a key, a person can not only jeopardize their data, but also data which, in case of loss, pose a great danger to the state as a whole. Such large-scale attacks are usually conducted and organized not by one person but by a group of hackers with the support of influential organizations, including security forces.

Information technology and telecommunication systems cover all spheres of human and state life. Almost every citizen uses cyberspace. And the faster humanity develops information technologies, the greater the need to protect information and telecommunication systems. Governments and communities around the world are looking for better measures and methods to protect their personal data from cyber threats.

A striking example of the importance of cyber security for the functioning of the state is a large-scale cyber-attack on corporate and state-owned networks using “NotPetya” virus, which took place on June 27, 2017. Such cyberattacks are aimed at destabilizing Ukraine. “Disable, destroy, destabilize” is their goal. Massive disconnections of electricity, telephone and Internet connections, difficulties in customer service and banking, real financial losses are what the enemy is using today.

Thus, the state needs rules, standards, regulations, regulations, instructions and other documents to ensure cybersecurity. Ukraine has developed security standards for critical infrastructure [10].

The basics of the national cybersecurity system are defined in the Law of Ukraine “On basic principles of cybersecurity of Ukraine” of 05.10.2017. No. 2163-VIII.

According to this Low, *the national cybersecurity system* is a set of subjects of cybersecurity and interconnected political, scientific, technical, informational, educational character, organizational, legal, operational-search, intelligence, counter-intelligence, defense, engineering and technical measures, and also measures of cryptographic and technical protection of national information resources, cyber defense of objects of critical information infrastructure.

*The main subjects of the national cybersecurity system* are the State Special Communications and Information Protection Service of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, the National Bank of Ukraine, which are in accordance with the Constitution and laws Ukraine performs the following main tasks in due course:

1) The State Special Communications and Information Protection Service of Ukraine ensures the formation and implementation of the state policy on cyberspace protection of state information resources and information, the requirement for protection of which is established by law, cybersecurity of objects of critical information infrastructure, exercises state control in these spheres; coordinates the activities of other cybersecurity entities; ensures creation and functioning of the National Telecommunication Network, implementation of organizational and technical model of cyber defence; carries out organizational and technical measures for prevention, detection and response to cyber incidents and cyberattacks and elimination of their consequences; informs about cyber threats and appropriate methods of protection against them; Ensures implemen-tation of information security audits on critical infrastructure, establishes requirements for information security auditors, determines the procedure for their certification (re-certification); coordinates, organizes and conducts security vulnerability assessment of communications and technology systems of critical infrastructure facilities; provides for the functioning of the State Cyber Security Center, the governmental CERT-UA computer emergency response team;

2) The National Police of Ukraine provides protection of human and citizen's rights and freedoms, interests of society and the state against criminal encroachments in cyberspace; undertakes measures for prevention, detection, termination and disclosure of cybercrime, raising awareness of citizens about cyberspace security;

3) The Security Service of Ukraine shall prevent, detect, suspend and open crimes against peace and security of humanity committed in cyberspace; carries out counterintelligence and search operations aimed at combating cyber terrorism and cyber espionage, implicitly checks the readiness of critical infrastructure facilities for possible cyber-attacks and cyber incidents; counteracts cybercrime, the consequences of which can threaten the vital interests of the state; investigates cyber-incidents and cyber-attacks on state-owned electronic information resources, information, the protection requirement of which is established by law, critical information infrastructure; provides response to cyber incidents in the field of national security;

4) the Ministry of Defence of Ukraine, the General Staff of the Armed Forces of Ukraine carry out, in accordance with their competence, measures to prepare the state for repression of military aggression in cyberspace (cyber defence); engage in military cooperation with NATO and other defence entities to ensure cyberspace security and joint protection against cyber threats; implement measures to ensure cyber defence of critical information infrastructure in a state of emergency and martial law;

5) Intelligence Agencies of Ukraine carry out intelligence activities on threats to national security of Ukraine in cyberspace, other events and circumstances related to the cybersecurity sphere;

6) The National Bank of Ukraine determines the procedure, requirements and measures for ensuring cyber defence and information security in the banking system of Ukraine and for the entities of funds transfer, supervises their implementation; creates a cyber defence centre of the National Bank of Ukraine, ensures the functioning of the cyber defence system in the banking system of Ukraine; provides assessment of cybersecurity and information security audit at critical infrastructure in the banking system of Ukraine [1].

One of the steps towards cyber defence at the state level was the Resolution of the Cabinet of Ministers of Ukraine dated 19.06.2019 "On approval of the General requirements for cyber defence of critical infrastructure facilities". Such facilities include enterprises, institutions and organizations whose activities are directly related to technological processes and/or the provision of services of major importance to the economy and industry, the functioning of society and the safety of the population, the disruption or disruption of which may to have a negative impact on the state of national security and defence of Ukraine, the environment, cause property damage and/or pose a threat to human life and health.

The said regulation stipulates that the organizational and technical measures for cyber defence should provide, in particular:

management of access of users and administrators to information security objects;

identification and authentication of users and administrators of information systems;

network protection of components and information resources;

availability and fault tolerance of information resources;

determining the conditions of use of variable (external) devices and storage media;

determining the terms of use of software and hardware [11].

It is also established that the owner and/or manager of a critical infrastructure facility must ensure that backups of information resources are promptly restored in the event of damage or destruction. In addition, the obligation of the owner and / or manager to inform the governmental CERT-UA Computer Emergency Response Team and the Security Service of Ukraine Cyber Security Situation Centre or a relevant unit of the SBU regional body is informed of cyber incidents and cyber-attacks. The said government decree also sets out a list of basic requirements for cyber defence.

## Conclusions

The analysis of trends in cyber security, considering the enhancement of the cyber security component in the national security system of the leading countries of the world, as well as the analysis of the scale of the effects of cyber-attacks on critical infrastructure has made the following conclusions:

cyber-operations are one of the most dangerous threats at the national level. Strategic enterprises, government agencies, and critical infrastructure sites may become targets for various cyberattack technologies;

modern and high-quality technical equipment is required to ensure the cyber security of the state and to keep it at an adequate level, as the development of one of the components of strategic communications;

cybersecurity is achieved through continuous work in the regulatory field, coordination of actions of state agencies in case of potential cyber-attacks, control over compliance with regulatory requirements for cybersecurity;

the education of security professionals must be constantly evolving, considering the latest technologies and experience of other countries.

## References

1. Law of Ukraine On the Fundamental Principles of Cybersecurity of Ukraine. Law of Ukraine dated 05.10.2017 No. 2163-VIII // Database "Legislation of Ukraine" / Verkhovna Rada of Ukraine. URL: http://zakon3.rada.gov.ua/ laws/show/984_001-16/paran2#n2 (accessed: 01/10/2019) [in Ukrainian]
2. Ordinance of the Cabinet of Ministers of Ukraine On approving the plan of actions for 2018 on implementation of the Cybersecurity Strategy of Ukraine of July 11, 2018 No. 481-p // Database "Legislation of Ukraine" / Verkhovna Rada of Ukraine. URL: http://zakon3.rada.gov.ua/laws/show/984_001-16/paran2#n2 (accessed: 01/10/2019) [in Ukrainian]
3. Network and information security: a proposal for a European policy approach: adopted by the European Commission on 6 June 2001 / European Union. URL: https://eur-

lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A52001DC0298 (accessed 01/06/2019)

4. About ENISA / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/about-enisa (accessed 01/05/2019)
5. Cyber Europe / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme (accessed 01/06/2018)
6. Council Framework Decision 2005/222 / JHA on attacks against information systems: adopted by the Council of the European Union on 24 February 2005 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32005F0222 (accessed 03/06/2018)
7. Towards a general policy on combating cybercrime: adopted by the European Commission on 22 May 2007 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=LEGISSUM%3Al14560 (accessed 02/06/2018)
8. Communication from the Commission on Critical Information Infrastructure Protection "Protecting Europe from a large scale of cyber-attacks and disruptions: enhancing preparedness, security and resilience": adopted by the European Commission on 30 March 2009 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52009DC0149 (accessed 04/06/2018)
9. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU: adopted by the European Commission on 13 September 2017 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=JOIN:2017:0450:FIN (accessed 05/06/2018).
10. State of the Union 2017 – Cybersecurity: Commission scales up the EU's response to cyberattacks: European Commission – Press release, 19 September 2017 / European Union. URL: http://europa.eu/rapid/press-release_IP-17-3193_en.htm (accessed 05/06/2018)
11. Zabara I.M. Formation of modern legal foundations of European Union cyber security in the conditions of diffusion of new innovative technologies. Journal of European and Comparative Law. 2017. Vol. 3. S. 2-13. [in Ukrainian]