Analysis of the ways of improvement of Ukraine – NATO cooperation on cybersecurity issues

Volodymyr Shypovskyi [A]; Volodymyr Cherneha [B]; Serhiy Marchenkov [C]

Received: April 1, 2020 | Revised: April 21, 2020 | Accepted: April 30, 2020

DOI: 10.33445/sds.2020.10.2.2

Abstract

Recent events in Ukraine have shown that, along with the advancement of information technology, methods of conducting modern warfare are being enhanced. Cyberspace is deliberately used by the Russian Federation to commit cyber warfare against Ukraine. Therefore, in order to address their influence effectively, it is important not only successfully deal with its consequences but also to foresee the potential adversary's actions by analyzing their previous operations and incorporating the lessons learned by other countries.

Across the globe, including Ukraine, the issue of information security and cyberattacks has become exceedingly urgent. Everybody is aware of the ongoing attacks on information networks of various government agencies and energy firms, cyberattacks on e-mail networks of political parties and organizations around the world. Likewise, despite the steadily growing numbers, cyberattack cases against the individuals and private businesses are not reported as widely as they occur.

As a result, The North Atlantic Alliance countries began tackling the issue of cyberthreats much earlier than Ukraine. Consequently, NATO and its allies rely on powerful and robust cyber defenses to ensure the Alliance's core tasks of collective defense.

The article discusses methods and strategies for providing cyber defense in NATO member states and recommends ways to increase the level of protection in the state's cyber space, as part of Ukraine's national security and defense domain.

Key words: cybersecurity, cybercrime, information war, cyberattack, cyberthreat, cyberspace.

Introduction

Today, the computerization of all spheres of society is one of the global determinants of human social, economic, intellectual and spiritual development. It is also important to recognize that humanity is entering a new era of development that can be characterized as a period of information and cyber wars. In particular, the information component is one of the key elements of the hybrid war against Ukraine, which is posing the real threat to national security since 2014. Thus, given the rapid formation and development of the information society in Ukraine, information security issues are of particular importance, specifically in the face constant threat of cyberattacks.

Material and methods

The advancement of digital technology and the pervasive penetration of telecommunications networks in almost all fields of human operation both encourage and complicate the

[A] The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Senior research officer of Research Section of the Educational and Research Center of Strategic Communications in the Sphere of National Security and Defense, Kyiv, Ukraine, e-mail: vladimir.shipovsky@gmail.com, ORCID: 0000-0003-3743-3064

[B] The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Ph.D in Technical Science, Docent of Department of Information Technology and Information Security Employment, Institute of the Troops (Forces) Support and Information Technologies, Kyiv, Ukraine, e-mail: chevn1980@gmail.com, ORCID: 0000-0016-1903-3252

[C] Zhytomyr Military institute, Head of Department of Information Warfare, Zhytomir, Ukraine, e-mail: marchenkov1978@ukr.net, ORCID: 0000-0003-4597-3618

creation and storing of databases, the automated processing of information, and the capacity to instantaneous information transfer around the world. This concerns the need to build secure environments for the use of virtual space, including protection against the dangers posed by criminals. The further development of the use of computer technology offers new possibilities for committing conventional crimes and establishes the conditions for the introduction of radically new schemes and methods of illegal activity. The importance of counteracting the use of information technology in illegal activities at this stage of the growth of the Ukrainian state is undeniable. Furthermore, the degree of computerization and the amount of incentives offered by intruders, and the propensity to increase cybercrime, pose a threat to Ukraine's democratic transformation and national security.

Analysis of recent research and publications. The findings of the review of specialized literature show that there is large number of works on particular aspects of fighting cybercrime and maintaining cyber security in Ukraine. Specifically, the concerns posed by A. Abramov, R. Gryshchuk, Y. Danik, V. Vekhov and others were studied these issues. Meanwhile, the rapid growth of computing technology and the complexities of the cybercrime advocate that some of their first "consumers" are offenders. In addition, the method of identifying and addressing cybercrime and its effects characterized by its complexity and needs continuous improvement.

The purpose of the article is to explore the legal framework and the current state of cyber security in Ukraine, particularly in the national security and defense domain: to identify the shortcomings of cyber security and information protection, to compare the efficacy of some aspects of the NATO Cyber Protection Doctrine, and to explore the possibilities and potential benefits of deepening Ukraine-NATO cooperation in Cybersecurity domain.

Results and discussion

The rapid growth of information technology, computerization and the emergence of a global digital space have created radically new substances-information society, cyberspace, which have an inexhaustible capacity and plays a major role in the economic and social growth of the countries of the world. Nevertheless, the emergence of an information society has led to increasing numbers of cyber threats, and thus the one of the main challenges of today's information society is to ensure security in cyber domain.

Consequently, countering risks to national security and the cyberspace defense industry has taken on a new scope today. Cyberattacks are becoming more organized, coordinated and disruptive to the economy and critical infrastructure of government agencies and corporations, so they can reach a critical level which threatens national and Euro-Atlantic prosperity, security and stability. Adversary military and intelligence forces, organized crime organizations, terrorist and extremist organizations are the potential beneficiaries of existing vulnerabilities.

Under these conditions, the key challenge of European and other countries of the world is to take steps that drastically minimize (and, in some cases, eliminate) the negative effects of cyberattacks. The North Atlantic Treaty Organization (NATO) plays a significant role in establishing a cohesive approach to information security as part of national security. The range of potential uses of cyber technologies presents one of the main challenges for NATO considering its role in providing cyber security to Allies and Partners. Admittedly, given the potential damage of cyber threats to national security, the cyber defense has now become one of top NATO's priorities.

The new NATO Strategic Defense and Security Framework adopted by the Heads of State and Government at the NATO Summit on 19 November 2010, effectively leveled cyber threats to military force, which, in turn, allows for a comprehensive cyberattack through the use of national armed forces. Cyber threats have become one of the most critical security challenges facing the Allies, and cyber security has been described

as the second most significant NATO priority. NATO's Cyber Security Policy, in effect, states cooperation with partner countries in developing an Alliance cyber protection network as a key mechanism for NATO's cyber security efforts [1].

The status of the Alliance was endorsed in the Declaration of the Chicago Summit, endorsed by the Heads of State and Government who attended the North Atlantic Council meeting in Chicago (USA) on 20 May 2012 [2]. In particular, paragraph 49 of the Declaration refers to NATO's readiness to collaborate with international partners to coordinate and ensure effective responses to cyber threats.

The final recognition of the Cyberspace Alliance as an operational area for warfare was the result of the NATO summit held in Warsaw (Poland) on 8-9 July 2016 [3].

The role of NATO in cyber security can be divided into two specific components. The goal is the security of their networks, which was decided by the Allies at the NATO Summit in Newport, Wales, on 4-5 September 2014. Given the Alliance's widespread presence on the Internet, this role is too difficult. Consequently, NATO must secure all information and communication systems that are crucial for Alliance operations and missions in cyber domain.

The second goal of NATO is to support its member countries in improving of their cyber defense capabilities. This effort is achieved by a number of ways, including a two-year method, to define the common goals of cyber security that each member of the Alliance will support, such as the implementation of a cyber defense strategy. The plan to achieve these mutually agreed goals is reviewed on a regular basis. NATO also provides a wide range of educational and training programs through a number of educational institutions, including the NATO School in Oberammergau (Germany) and the Cyber Academy, founded in Portugal. The NATO-accredited Cooperative Center for Cyber Defense Excellence in Tallinn, Estonia, also plays a significant role in this regard.

The activities of NATO must be mutually reinforcing. The security of the Alliance and its ability to fulfill the agreed collective defense mission depends to a large extent on the cyber defense capabilities and capabilities of each NATO member country[4]. Establishing a national cyber security infrastructure capable of counteracting cyber threats to national security is an important problem facing Ukraine today. The state of cyber security in Ukraine indicates that cyberspace remains a significantly vulnerable part of national security and remains highly susceptible to cyber threats.

Following international agreements, Ukraine cooperates in the area of informational security with foreign nations, their military forces, law enforcement agencies and special services, as well as with international organizations. Thus, Ukraine's strategic relationship with the North Atlantic Treaty Organization supports the objectives of international cyber security cooperation.

In January 2008, NATO adopted the Alliance's cyber policy framework, recognizing the effect of cyber-attacks on Estonia in October 2007, when government websites and other Estonian communication networks were disrupted. This led to a concerted effort by all NATO countries to improve cyber defense and information security. Consequently, NATO allies agreed on Memorandum to create an international NATO information defense center in Tallinn (Estonia).

In 2008, on the initiative of the Security Service of Ukraine, NATO-Ukraine Joint Working Group on Military Reform set up a working sub-group on cyber defense. This sub-group provided an impetus for the establishment of conceptual mechanisms for cooperation between Ukraine and the North Atlantic Alliance in consultation and exchange of information on cyber security. In 2009, the Alliance adopted a strategic document, "A Framework for Cooperation on Cyber Security between NATO and Partner Countries", which established a political and legal framework for collaboration and cooperation with partner countries, including Ukraine. The key objectives of cooperation between NATO and its partners in the field of cyber security are: to ensure the normal functioning of critical information and communication infrastructures; to establish effective measures to combat cyberattacks; to assist countries in restoring the proper functioning of the related infrastructure as a result of external

cyber-attacks; implementation of a mechanism of prompt response to cybersecurity threats.

Presidential Decree No. 744/2014 of 24 September 2014 put into force the decision of the National Security and Defense Council of 28 August 2014 on urgent steps to protect and improve Ukraine's defense capability, which states that Ukraine's priority national interest in foreign policy is to further establish Ukraine's strategic partnership with the US, the EU and NATO [5].

Following the decision of the National Security and Defense Council of Ukraine on the National Security Strategy of Ukraine of 6 May 2015, adopted by Presidential Decree No. 287/2015 of 28 May 2015, ensuring Ukraine's entry into the EU and establishing the conditions for NATO membership are the key priorities of modern defense policy [6]. One of the main challenges to national cyber security is the insecurity of Ukraine's vital infrastructure and public information systems.

Consequently, the National Cyber Security and Cyber Risk Response Center was established in Ukraine on 1 July 2015 to support the Computer Emergency Response Team of Ukraine (CERT-UA). The Center shall serve as the Technical Coordinator of State governments, local self-government entities, military agencies, businesses, organizations and organizations, regardless of the mode of ownership for the prevention, identification and elimination of cyber incidents.

The establishment of safe, stable and secure cyberspace and the strengthening of Ukraine's cooperation with NATO to improve Ukraine's information security capabilities are supported by the decision of the Ukraine's National Security and Defense Council On Ukraine's Cyber Security Policy of 26 January 2016, adopted by Presidential Decree No 96/16 of 15 January 2016 [7].

In the framework of the agreements reached between Ukraine and NATO, a joint decision was taken to set up five trust funds for our country, with the fifth fund designed to fight cybercrime and to build cyber defense systems in line with the most progressive standards of NATO member countries. Estonia, Romania, Turkey and Hungary have contributed to the Campaign. The concept behind the formation of the NATO-Ukraine Cyber Security Trust Fund is that its intellectual and material capabilities would provide Ukraine with the requisite support solely for the advancement of defense technological capabilities, including the establishment of cyber incident investigation laboratories. The main goal of this Trust Fund initiative is to coordinate NATO member countries to support Ukraine in developing its cyber security capability by providing hardware and software, software, technical assistance, advisory services and training.

The NATO Trust Fund offers an opportunity to boost the level of cyber security in Ukraine by consulting information security experts, developing the basic principles of the National Cyber Security Framework, working in NATO-Ukraine expert level boards in cyber security area.

On 24 September 2015, the President of Ukraine approved the resolution of the National Security and Defense Council of Ukraine On a New Version of the Military Doctrine of Ukraine No. 555/2015 [8]. This decree lays down the conceptual foundations of the state's military strategy and the current framework for responding to Ukraine's national security threats. Specifically, paragraph 59 of the War Doctrine states the need to strengthen collaboration and collaboration with NATO and the EU by obtaining access to their intelligence knowledge networks in order to ensure an efficient and coordinated response to cybercrime attacks.

Ukraine is therefore consolidating its efforts on implementation of NATO standards to be fully integrated to the global cyber defense framework. Nevertheless, the process of joining the collective security system is still slow, indicating that the current cyber capabilities not in line with NATO requirements [9].

Conclusions

The analysis of NATO policies, in relation to integration of Ukraine's cyber security component to Euro-Atlantic structures, leads toward following conclusions:

Ukraine needs a cyber security system interoperable with NATO-EU partners, the protection in cyberspace is an integral part of national security.

On the one hand, Ukraine is improving its own cyber defense through the use of NATO's Information Security Trust resources, and on the other, such collaboration is advantageous to the Alliance because it offers real world and real time technological and organizational verification and validation mechanism of its concepts and doctrines.

Considering the significant progress and expertise of NATO in establishing and strengthening the cybersecurity mechanism of the Member States, Ukraine must become an active participant in these security processes. Thus, considering Ukraine's Euro-Atlantic ambitions, it will help to boost the reputation of the country and on the other hand, to establish the legal basis of national cyber security. Likewise, it facilitates the integration to NATO and development of an optimal model for the secure defense of domestic cyberspace. In the face of hybrid warfare and the implementation of e-governance activities, aspects of cybersecurity for Ukraine should be the subject of public policy.

References

1. Relations with Ukraine / The North Atlantic Treaty Organization's official website. URL: https://www.nato.int/cps/en/natolive/topics_37750.htm (accessed 12/01/2020)
2. Speech by NATO Secretary General Anders Fogh Rasmussen to the chairpersons of the foreign affairs committees of the European Union member's states parliaments, Copenhagen (12 March 2012) / NATO multimedia library. URL: http://www.natolibguides.info/nato-eu/documents (accessed 11/12/2019)
3. Defending against cyber attacks / The North Atlantic Treaty Organization's official website. URL: https://www.nato.int/cps/en/natohq/topics_118663.htm?selectedLocale=en (accessed 14/02/2020)
4. The Cyberpolice of Ukraine. Diskcoder. C virus was the cover up for the largest-scale cyberattack in the history of Ukraine. URL: https://cyberpolice.gov.ua/news/prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/. (accessed 10/02/2020) [In Ukrainian]
5. Ukrinform (2017) The Ministry of Defense has successfully repelled the cyberattack. Multimedia broadcasting platform of Ukraine. URL: https://www.ukrinform.ru/rubric-society/2256867-v-ukraine-sozdaut-kibervojska-poltorak.html. (accessed 09/11/2019) [In Russian]
6. On approval of the plan of actions for 2018 on implementation of the Cybersecurity Strategy of Ukraine / Legislation of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80 (accessed 09/03/2020) [In Ukrainian]
7. On approval of the action plan for 2017 on the implementation of the Cybersecurity Strategy of Ukraine / Legislation of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80 (accessed 24/03/2020) [In Ukrainian]
8. On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cybersecurity Strategy of Ukraine" Legislation of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80 (accessed 24/03/2020) [In Ukrainian]
9. Dubov D. Cyber space as a new dimension geopolitical rivalry. Monograph. 2014. 328 pp.