IMPROVING UKRAINE'S ADMINISTRATIVE-LEGAL SUPPORT FOR CYBER SECURITY: EU AND NATO EXPERIENCE IN COUNTERING HYBRID CYBER THREATS

Liliya Veselova[1]

[1]*Ph.D. (Law), Odessa State University of Internal Affairs, Odessa, Ukraine, e-mail: cvet-Liliya@ukr.net, ORCID: https://orcid.org/ 0000-0001-6665-0426*

Abstract. *The article focuses on the activities of NATO and the European Union, that consider combating hybrid threats a priority for international cooperation. A number of EU documents have been analyzed, which form a clear idea of cyber threats' hybridity and main directions of administrative, legal and organizational support of cybersecurity, in particular, on combating hybrid cyber threats in the European Union. Based on the analysis, that at the present stage of development of society the bases were formed on the establishment of a sustainable perception of the risk problem as one of the forming factors of the modern and especially the future society, which is also becoming increasingly socially important. The aim of the article: to identify areas for improving the administrative and legal support of cybersecurity in Ukraine by borrowing the experience of the EU and NATO to combat hybrid cyber threats. The research methodology: the system of general scientific and special methods of cognition, namely the formal-legal method, comparative legal method and method of scientific abstraction. It is emphasized that the domestic regulatory framework has significant shortcomings and requires the introduction of appropriate rules for the introduction of risk-based approach in cybersecurity activities in Ukraine, as well as the definition of basic terms («risk-based approach to cybersecurity», «risk-oriented approach to critical infrastructure protection», «risks», «risk management»). The essence and meaning of the term «sustainability», which has gained practical application in strategic documents in the field of security and in essence is the latest concept of modern theory of national security, which has practical significance for state policy in security environment and is important for security practice in cyberspace, because it is the presence of hybrid threats in cyberspace that cannot be prevented, necessitates the formation of a new approach, in particular, the formation of «sustainability», which in turn should be implemented in public cyberspace policy.*

Keywords: *cyberattacks, cybersecurity, hybrid war, resilience of society, response, risks.*

JEL Classification: F52, H55, H56, K22, K33

Formulas: 0; fig.: 0; tabl.: 0; bibl.: 9

Introduction. Today, in the context of the hybrid war, which has been actively imposed on Ukraine since spring 2014, cybersecurity is extremely important, as cyberattacks, which are actually an escalation of hostilities in cyberspace, spread the latest forms of aggression and increase threats to citizens and society and in some cases cause real damage to the state.

Literature review. The issue of cyber security and public policy aimed at its provision has been the subject of research by many leading scholars in the field of administrative, constitutional and other related areas of law, including: V.B. Averianov, I.V. Aristova, I.L. Bachylo, I.P. Holosnichenko, O.D. Dovhan, R.O. Dodonov, I.M. Doronin, L.V. Kuzenko, O.Ie. Kutafin, V.L. Manilov, O.V. Nesterenko, H.V. Padalko, V.P. Pietkov, S.V. Pietkov, V.L. Sydorenko, O.Iu. Syniavska, S.H. Stetsenko, V. Tertychko, M.M. Tyshchenko, Yu.P. Tykhomirov,

O.M. Shevchuk, V.K. Shkarupa and other, but also on improving the administrative and legal support of cybersecurity in Ukraine through EU and NATO experience in combating hybrid cyber threats still remain insufficiently addressed.

Aims. The aim of the article is to identify areas for improving the administrative and legal support of cybersecurity in Ukraine by borrowing the experience of the EU and NATO to combat hybrid cyber threats.

Methods. The methodological basis of the study is a system of general scientific and special methods of cognition, namely the formal-legal method, comparative legal method and method of scientific abstraction.

Results. Hybrid threats are aimed at exploiting the vulnerabilities of countries and are aimed at undermining fundamental democratic values and freedoms. The West's approaches to awareness of hybrid threats are based on countermeasures: the EU focuses on cybersecurity, countering organized crime, risk neutralization, strengthening the resilience of society, and information security.

NATO and the EU have a clear understanding that hybrid threats need to be prevented as «passive» elements, such as enhancing resilience to shocks or surprises, and more proactive, including strong measures to prepare and protect the functions and structures most likely to be targeted at hybrid attacks. In this context, it is impossible to exaggerate the importance of active action to strengthen civic preparedness, free press, an educated population and an effective legal structure [1].

The allocation of certain measures in the direction of counteracting hybrid threats clearly demonstrates the priority formed in the EU.

Further development of the cybersecurity system in the EU is quite thoroughly characterized in the final documents, which were issued in the form of:

–joint communiqués of the European Parliament and the European Council on the implementation of measures to combat hybrid threats in the European Union, in particular: 06.04.2016 [2]; 19.07.2017 [3]; June 13, 2018 [4];

–the report on implementation of the 2016 action plan to combat hybrid threats and the Joint Communication of 2018 on increasing resilience and strengthening opportunities to overcome hybrid threats from 28.05.2019 [5].

The general analysis of these EU documents forms a clear idea of hybridity of cyber threats and the main directions of administrative-legal and organizational support of cybersecurity, in particular, the fight against hybrid cyber threats in the European Union.

The main purpose of these annual reporting documents is to present a report to the European Community on the progress and next steps in implementing the actions in the four areas proposed in the Joint Activities: raising awareness of the situation: sustainability of society; strengthening the capacity to prevent and respond to crises, and coordinating the resumption and expansion of cooperation with NATO to ensure complementarity in activities.

In developing awareness-raising on hybrid cyber threats, the emphasis is on identifying societal vulnerabilities to them and coordinated action to assess these threats. To identify key vulnerabilities, taking into account specific hybrid indicators, an analysis of risks affecting institutions and networks is carried out.

With regard to the risk-based approach, it is appropriate to note the adoption of Resolution 57/239 «Elements for a Global Cyber Security Culture» [6] by the UN General Assembly on 20 December 2002, according to which the term «cybersecurity» has been actively used in legal terminology. It is significant that back in 2002, UN documents indicated the need to assess risks in order to identify threats and vulnerabilities.

Therefore, the global culture of cybersecurity involves nine interrelated elements, including:

– awareness (that is, participants need to be aware of the need for security of information systems and networks, and what they can do to increase security);

– responsibility (participants are responsible for network security according to their own role);

– response (participants should take timely and joint measures to prevent, detect and respond to security incidents, including the exchange of information and procedures that provide for prompt and effective cooperation in preventing, detecting and responding to such incidents); ethics (taking into account the legitimate interests of others);

– democracy (security must be ensured in a way that is consistent with democratic values, including the freedom of exchange of views and ideas, the free flow of information, confidentiality of information, proper protection of private information; openness and transparency); risk assessment (participants should carry out periodic risk assessments to identify threats and vulnerabilities, have appropriate technologies and control tools for this purpose, taking into account the importance of information being protected);

– design and implementation of security measures;

– reassessment (appropriate and timely measures to make changes in policy, security practices taking into account new and changes in existing threats) [7, p. 72-73].

The UN resolution is not the only international legal instrument that emphasizes the need to assess risks in the cybersecurity system. In particular, the EU Directive on measures to ensure a high general level of security of network and information systems throughout the Union (NIS Directive) [8] lays down uniform rules and requirements in the field of cybersecurity for all EU countries, but leaves each Member State the right to take its own measures concerning the implementation of this Directive's provisions into national law. Moreover, the Directive required Member States to implement these rules before 9 May 2018.

This implies that in order to increase the capacity to provide cybersecurity at the national level, EU Member States should develop a national network and information

security strategy, which should include: strategic goals, priorities and the state basis; measures to prepare for, respond to and recover from cyber incidents, principles of public-private partnership; a program of educational, training and awareness-raising activities; research plan; risk assessment and management plan; a list of stakeholders responsible for implementing the strategy; identify one or more public authorities that will be responsible for implementing the Directive; create one or more computer emergency response teams.

In general, in order to achieve the goal of the Directive, to ensure a higher level of network and information security within the European Union, three main areas have been identified as necessary measures: increasing the capacity of the cybersecurity system at the national level; raising the level of pan-European cooperation; introduction of risk management and the obligation to report cyber incidents to basic service operators and digital service providers.

Thus, risk management is defined by international law not only as a recommendation, but also as a mandatory element that raises awareness of vulnerability of the system in the field of cybersecurity.

To understand the problems that occur in the field of cybersecurity, as well as finding ways to solve them, it is important to study the history and logic of the concept of «risk» origin, its essence, content and place in modern social development.

In general, it should be noted that the development of society in a fairly long historical period, in some ways, was marked by risk. At the same time, a relatively new product of scientific thought development was the awareness of human activity's riskiness and the risk attributiveness in the processes of modern social development.

An important task is to clarify the possibilities of public management of social risks of information society development in Ukraine.

An important element of further development of Ukraine's cybersecurity system, especially in a hybrid war, is the need to implement the provisions of European Parliament and Council Directive (EU) 2016/1148 of 6 July 2016 on measures for a high common level of security of network and information systems in the Union (hereinafter – the NIS Directive) [9].

The provisions of this NIS Directive contain a number of requirements to improve the level of cybersecurity. In particular, national cybersecurity strategies address the following issues: goals and priorities of the national strategy for network and information systems security; governance framework to achieve the goals and priorities of the national strategy for the security of network and information systems, including the roles and responsibilities of government bodies and other relevant actors; identifying tools for preparedness, response and restoration, including cooperation between the public and private sectors; indicating educational, training, and awareness-raising programs related to the national strategy for the security of network and information systems; indication of research and development plans related to the national strategy for the network and information systems' security; risk assessment plan to identify risks; a list of various actors involved in the

implementation of the national strategy for the security of network and information systems.

In addition, in Art. Articles 14 and 16 of the first security and incident reporting requirement state that Member States shall ensure that basic service operators as well as digital service providers take appropriate and proportionate technical and organizational measures to manage network and information security risks systems they use in their operations. Given the latest knowledge, such measures should ensure a level of security of network and information systems that corresponds to the risk that has arisen.

In general, the text of the NIS Directive uses the term «risk» 17 times, which in Art. 4 «Terms and definitions» is defined as follows: «risk» means any circumstance or event that can reasonably be identified that has the potential to adversely affect the security of network and information systems [9].

Therefore, it should be noted that in connection with implementation of European legislation in Ukraine, we will be forced to implement these provisions of the NIS Directive to domestic legislation.

Discussion. The current Law of Ukraine «On Basic Principles of Cyber Security of Ukraine» does not provide for any activities to assess risks in the field of cyber security. In our opinion, this is a significant shortcoming of the current domestic legislation, which is motivated by us from several points of view:

–objectively, modern processes of social development require the introduction of the institute of scientific forecasting in management decisions, the provision of which is methodologically in security plane and is based on a risk-oriented approach to forecasting;

–risk assessment in the field of cybersecurity of Ukraine is not only a necessity of the current stage of development of society, but also a requirement of formal and legal international legislation, in particular, European, the further implementation of which in Ukraine requires implementation and enforcement;

From a methodological point of view, risk assessment involves not only informing about the magnitude of a threat in cybersphere, but also clarifying the resilience of society in combating these threats, which therefore forms the basis for identifying priorities for improving the resilience of cybersecurity's domestic system of Ukraine;

The current state of cybersecurity in Ukraine directly depends on aggressor's activity in cyberspace, and therefore cyber threats to our society, above all, do not lie in the plane of internal factors, but only - external targeted activities of the aggressor's intelligence services, which objectively motivates an effective national cybersecurity system in Ukraine;

Given the place of the institution of risk-oriented approach (risk assessment, risk management) in the mechanism of state regulation, it is objective to implement it in current legislation and identify an important tool in the mechanism of administrative-legal regulation as a preventive measure.

Conclusion. Thus, the current domestic legislation requires the introduction of appropriate rules for the introduction of a risk-oriented approach in cybersecurity activities in Ukraine. In particular, this applies to both the Law of Ukraine «On Basic Principles of Cyber Security of Ukraine» and the draft Law of Ukraine «On Critical Infrastructure and its Protection» of 27.05.2019 № 10328-III. In particular, innovation of this content should contain the following:

Definition of basic terms: risk-oriented approach to cybersecurity - the principle of cybersecurity, based on assessing the risks of violations of rights and freedoms, as well as the interests of society and the state in cyberspace, and taking appropriate risk management measures in a way and to the extent minimization of such risks depending on their level; risk-oriented approach to critical infrastructure protection - the principle of critical infrastructure protection, based on risk assessment of critical infrastructure security breaches, as well as taking appropriate risk management measures in a manner and to the extent that minimizes such risks depending on their level; risks - the real threat's level of violation of rights and freedoms, as well as the interests of society and the state in cyberspace (violation of the security of critical infrastructure); Risk management - a set of measures taken by cybersecurity entities (critical infrastructure operators): identification and assessment of threats and vulnerabilities of the national cybersecurity system (critical infrastructure), risk assessment of threats - and on this basis to make appropriate management decisions to minimize risks.

References:

1. Spivpratsia zarady protydii hibrydnym zahrozam [Cooperation to counter hybrid threats]. URL: https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozam/index.html [Ukraine].

2. Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

3. Joint Report to The European Parliament and the Council on the Implementation of the Joint Framework on countering hybrid threats - a European Union response. 2017. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017JC0030.

4. Joint Report to the European Parliament, the European Council and the Council on the Implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2018:014:FIN.

5. Joint Staff Working Document Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. URL: https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf.

6. UN General Assembly resolution 57/329, adopted at the 78th plenary session of the 57th session. 20.12.2002. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement.

7. Dovhan O.D., Doronin I.M. (2017) Eskalatsiia kiberzahroz natsionalnym interesam Ukrainy ta pravovi aspekty kiberzakhystu [Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber defense], Kiev, 107 p. [Ukraine].

8. Propozytsii do polityky shchodo reformuvannia sfery kiberbezpeky v Ukraini. [Proposals for policy on cybersecurity reform in Ukraine]. *Material dlia obhovorennia [Material for discussion]*. URL:

https://parlament.org.ua/wp-content/uploads/2017/12/au_White-book-on-cybersecurity-draft_5.pdf [Ukraine].
9. Dyrektyva Yevropeiskoho Parlamentu I Rady (IeS) 2016/1148 vid 06.07. 2016 pro zakhody dlia vysokoho spilnoho rivnia bezpeky merezhevykh ta informatsiinykh system na terytorii Soiuzu [Directive of the European Parliament and of the Council (EU) 2016/1148 of 06.07. 2016 on measures for a high common level of security of network and information systems in the Union.]. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA [Ukraine].

Received: August 08, 2020
Approved: September 22, 2020