LEGAL PRINCIPLES OF CYBER PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES

Volodymyr Shablystyi, Dnipropetrovsk State University of Internal Affairs
Vitaliy Prymachenko, Dnipropetrovsk State University of Internal Affairs
Anastasiia Filipp, Dnipropetrovsk State University of Internal Affairs
Lina Doroshenko, Donetsk National University
Vitaliy Burbyka, Sumy State University

ABSTRACT

The paper explores the legal foundations of cyber protection of critical infrastructure. To this purpose, the essence of the cyber protection concept has been established by elucidating of scientists' positions in defining this term. The peculiarities of the legal regulation of cyber protection of critical infrastructure facilities in the leading countries of the world (case study of UK and USA) have been considered and the bodies which act at the state level in this direction have been identified. The content of the norms of some Ukraine's regulations were considered, which regulate the issues of cyber protection of critical infrastructure facilities, in particular, criteria and the order of objects assignment to critical infrastructure facilities, a list of such objects, general requirements for their cyber protection, etc. Particular attention is focused on the basic requirements for cyber protection of critical infrastructure.

Keywords: Cyberspace, Cyber Security, Cyber Protection, Cyber Incident, Cyber Threats.

INTRODUCTION

The modern, fast-paced processes of informatization of the global scale, on one hand, open new opportunities for the development of all spheres of the society, and on other hand they cause new threats to the national security of a state. Emergence of cyberspace (virtual space) as a separate dimension of human existence and development caused not only transformation of social relations in a positive direction, but also new challenges and threats. The priority for any country in this context is formulation and effective implementation of cybersecurity policy, creation and improvement of the cyber protection systems of critical infrastructure facilities from external and internal cyber threats.

Statement of the Problem

The introduction of information and communication technologies into the critically important spheres of the society life and a state, and the emergence of cyber threats require the development and implementation of cyber security measures which advance to the interstate level. Therefore the nationwide cyber security systems have been already formed in many of the world's leading countries. Formation of a cyber security system is also taking place in Ukraine. In this regard, it is important to identify the features of cyber protection of critical infrastructure

facilities in accordance with current Ukrainian legislation and to explore the foreign experience of the leading countries in the legal regulation of these issues.

LITERATURE REVIEW

Establishing the legal principles of cyber security of critical infrastructure facilities requires the definition of cyber security. A lot of scientists paid attention to the study of this issue. Researchers' positions in defining the cyber protection are diverse. Thus, the authors Galinec et al. (2017) define the cyber security as a mechanism for protecting a computer network, which includes responding to actions, protecting critical infrastructure and providing information to organizations, government agencies and other possible networks. Cyber security is focused on preventing, detecting and providing timely reactions to attacks or threats in order not to counterfeit the infrastructure or information. Taking into account the increasing volume and cyber-attacks complexity, the cyber security is essential for the most organizations for protecting sensitive information as well as assets protect. In this way, the cyber protection helps to increase the efficiency and cost of security resources. Dewar (2014) reveals the essence of the cyber protection concept by dividing it into active and passive types. According to the researcher, active cyber protection characterizes taking actions for counteraction the immediate effects of cyber incidents, detecting and neutralizing malware, masking the presence of target devices for deterrence and counteracting espionage in the Internet. The active cyber protection is relevant to banks in the context of informatization of the financial space, special attention should be paid to developing a mechanism for monitoring banking transactions that are most vulnerable to cyber-attacks and use for crime financing (Leonov et al., 2019). In contrast to the active cyber protection, the passive one aims to address cyber incidents as soon as it happened, rather than actively trying to prevent them. Chen (2017) draws attention to such a feature of cybersecurity as dynamic, justifying the imperfection of modern approaches to such protection of cyberspace because of their general static nature.

METHODOLOGY

Legal principles for cyber protection of critical infrastructure were identified using dialectical, formal-juridical, and comparative-legal methods. The dialectical method was applied to establish the essence of the cyber protection concept by illuminating scientists' positions in defining this term. The formal-juridical method allowed revealing the content of the norms of some current regulations of Ukraine, which regulate the issues of cyber protection of critical infrastructure facilities, in particular, criteria and the order of objects assignment to critical infrastructure facilities, a list of such objects, general requirements for their cyber protection, etc. The use of the comparative-legal method was aimed to highlight the specific legal regulation of cyber protection of critical infrastructure facilities in the leading countries of the world and to determine the bodies which act at the state level in this direction (case studies of the UK and USA).

FINDINGS AND DISCUSSIONS

Great potential in cyber protection sphere is characterized for the UK, where the Government Communications Headquarters (GCHQ)[1] functions effectively. GCHQ provides

intelligence, protects information and informs relevant UK policy to keep society safe in the Internet epoch. In terms of cyber security GCHQ aims to create the conditions which enable the UK to be the safest place for living and doing business on the Internet. The GCHQ's opportunities are the following:

1. Collection: A number of methods are used in strict compliance with norms of acting law to collect messages and data which are important;
2. Analysis: Communications and data are analyzed to generate intelligence reports;
3. Effects: The use of variety online opportunities can lead to a real world result (The official website of GCHQ).

The National Cyber Security Center (NCSC) as a part of the GCHQ structure was created with the purpose of cyber protection of the critical infrastructure facilities. NCSC provides advice, guidance and support on cybersecurity, including management of cyber security cases to facilitate industry-government interaction. NCSC supports major UK organizations, general public sector, industry and the general public. In the event of cyber incidents, the NCSC provides an effective response to it to minimize damage to the UK and to draw conclusions for the future. NCSC collaborates with the UK's law enforcement, defense, intelligence, security services and international partners[2].

In order to regulate cyber protection of critical infrastructure facilities, the Cyber-Attacks (Asset-Freezing) Regulations was adopted in the United Kingdom on May 20, 2019, published on the official website www.legislation.gov.uk together with an explanatory memorandum. Support of social cohesion in society, ensuring competitiveness, sovereignty and entry into the world economy system are the priorities of any country's economic security (Reznik & Shevchenko, 2015). In this regard, the measures implemented include freezing the funds and economic resources of any persons and entities listed in Annex I of the Regulation and ensuring that the funds and economic resources are not provided to them or for their benefit (The Cyber-Attacks Asset-Freezing Regulations, 2019).

The critical infrastructure describes physical and cyber systems and assets in the United States which are so vital important to the United States that their incapacity or destruction would have a profound effect on economic security or public health. The critical infrastructure of the country provides the most important services that underpin American society (The official website of the Department of Homeland Security)[3]. The legal principles for cyber protection are centered in the National Cyber Strategy of 2018 (National cyber strategy of the United States of America, 2018).

The Law "*On the Cyber Security and Infrastructure Security Agency*" was adopted in 2018. The Cyber Security and Infrastructure Security Agency (CISA) coordinates security and resilience efforts through strong partnerships in the private and public sectors, and provides technical assistance and evaluation to federal stakeholders, as well as infrastructure owners and operator through all country. The main activities of CISA to ensure the security of critical infrastructure facilities are:

1. Provision of free tools and resources to public and private partners;
2. Facilitating the assessment of critical infrastructure vulnerabilities;
3. Enhanced security and resilience in the chemical sector;
4. Providing training, promoting information sharing and facilitating industry partnerships and international engagement (Cybersecurity and Infrastructure Security Agency Act, 2018).

CISA works with business, communities and government at all levels to make the country's critical infrastructure more resilient to cyber threats[4].

The National Risk Management Center (NRMC) was created within the framework of CISA. This is a center of planning, analysis and cooperation, which works to identify and address the most significant risks to our country's critical infrastructure. NRMC works closely with the private sector and other key stakeholders in critical infrastructure to: analyze; set priorities; and manage the major risks to national critical functions-government and private sector functions are so vital important to the United States that their destruction, corruption or dysfunction will have a profound effect on national economic security, national health (The official website of CISA).

Taking into account the practices of the leading EU countries and USA on the issues of cyber protection ensuring in cyberspace, the Law *"On Basic Principles of Cyber security of Ukraine"* (hereinafter-the Law) was adopted in Ukraine on October 5, 2017. According to Article 1 of the Law the concept of cyber protection defines as a set of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical protection of information aimed at preventing cyber incidents, detecting and protecting against cyber-attacks, eliminating their consequences, restoring the sustainability and reliability of functioning systems of communication technological systems (Law of Ukraine, 2017).

In accordance with Part 1 of Art. 6 of the Law the critical infrastructure facilities include enterprises, institutions, and organizations, regardless of ownership, which meet certain criteria. In particular, they:

1. Operate and provide services in the energy, chemical industry, transport, information and communication technologies, electronic communications, banking and financial sectors;
2. Provide services in the areas of population vital activity, in particular in the areas of centralized water supply, sewerage, electricity and gas supply, food production, agriculture, and health;
3. They are communal, emergency and rescue services, population emergency medical services;
4. They are included in the list of enterprises of strategic importance for the economy and security of the state;
5. They are subject to potentially dangerous technologies and industries (Law of Ukraine, 2017).

According to Part 2 of Art. 6 of the Law, the Cabinet of Ministers of Ukraine approved the General Requirements for Cyber Protection of Critical Infrastructure Facilities on June 19, 2019 in order to establish criteria and order for the objects classification to critical infrastructure facilities, to determine the list of such facilities, general requirements for their cyber protection, including features of the cyber-threat indicators use. They were set basic requirements for cyber protection of critical infrastructure facilities. In particular, a critical infrastructure facility must have a unit or an officer responsible for information security policy adopted at the critical infrastructure facility and control for compliance with this policy. Some officers must also be assigned at the critical infrastructure facility that will be responsible for operation and information security of critical business/operational processes among the critical infrastructure facility's managers whose employees ensure the operation of these critical processes (General Requirements for Cyber protection of Critical Infrastructure Assets, 2019).

The working body of the National Security and Defense Council of Ukraine in the field of cyber protection is the National Cyber Security Coordination Center, which operates in accordance with the Regulation. One of the priorities of the National Cybersecurity Coordination

Center is the measures implementation to ensure cyber security of critical infrastructure facilities and technological processes protection in production in the real economy (Regulations on the National Cybersecurity Coordination Center, 2016).

RECOMMENDATIONS

One of the most dangerous institutional threats to Ukraine's national security remains corruption, which requires the state to develop measures to counteract this negative phenomenon (Reznik et al., 2019). Given this, cyber security can be an effective tool in detecting, preventing and combating corruption in cyberspace. Effectiveness of the use of the cyber protection means must be achieved not only through coordination between national cybersecurity authorities, but also at the level of global interstate communications.

CONCLUSION

In the context of cyberspace, it is necessary to develop and implement cyber security measures with the purpose to prevent cyber threats that may occur in it. That is why nationwide cybersecurity systems have been already formed in many of the world's leading countries. The Government Communications Headquarters (GCHQ) operates in the United Kingdom for this purpose. The National Cyber Security Center (NCSC), which is a part of the GCHQ structure, was created to protect cyber infrastructure facilities. The legal principle for cyber protection of critical infrastructure facilities in the UK is reflected in the Cyber Attack Regulation (assets-freezing). A cyber security agency in the United States is named as the Cyber Security and Infrastructure Agency, governed by the relevant Law. The legal basis for cyber protection of critical infrastructure facilities in Ukraine is the Law of Ukraine *"On Basic Principles of Ukraine's Cyber Security",* the Regulation on the National Cyber Security Coordination Center. One of the priority tasks of this authority is to take measures to ensure cyber protection of critical infrastructure facilities and technological processes protection in production in the real sector of the economy.

ENDNOTE

1. The official website of Government Communications Headquarters (GCHQ). Retrieved from https://www.gchq.gov.uk
2. The official website of National Cyber Security Centre (NCSC). Retrieved from https://www.ncsc.gov.uk/
3. The official website of the Department of Homeland Security. Retrieved from https://www.dhs.gov/topic/critical-infrastructure-security
4. The official website of CISA. Retrieved from https://www.cisa.gov/about-cisa

REFERENCES

Chen, J.Q. (2017). A new dynamic cyber defense framework. *International Journal of Cyber Warfare and Terrorism, 7*(4), 14-22.

Cybersecurity and Infrastructure Security Agency Act. (2018). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/3359

Dewar, R.S. (2014). The triptych of cyber security: A classification of active cyber defence. *6th International Conference on Cyber Conflict. NATO CCD COE Publications*.

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurityand cyber defence: National level strategic approach. *Automatika, 58*(3), 273-286.

General Requirements for Cyber Protection of Critical Infrastructure Assets. (2019). Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF

Law of Ukraine. (2017). *On the basic principles of ensuring cyber security of Ukraine: As amended up to Act of July 08, 2018*. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19

Leonov, S., Yarovenko, H., Boiko, A., & Dotsenko, T. (2019). Information system for monitoring banking transactions related to money laundering. *CEUR Workshop Proceedings.*

National cyber strategy of the United States of America. (2018). Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Regulations on the National Cybersecurity Coordination Center. (2016). *As amended up to Act of June 20, 2019*. Retrieved from https://zakon.rada.gov.ua/laws/show/242/2016

Reznik, O., & Shevchenko, H. (2015). Ensuring state economic security in the area of taxation: Agent-based and subject-based legal approaches. *Actual Problems of Economics, 6*(168), 162-172.

Reznik, O., Shendryk, V., Zapototska, O., Popovich, E., & Pochtovyi, M. (2019). The features of e-declaration as an effective tool to prevent corruption. *Journal of Legal, Ethical and Regulatory Issues, 22*(2), 1-9.

The Cyber-Attacks Asset-Freezing Regulations. (2019). Retrieved from https://www.legislation.gov.uk/uksi/2019/956/contents/made