ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.39 Nº 71
2021

Cuestiones Políticas Vol. 39, Nº 71 (2021), 789-799
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Protection of Critical Infrastructure Facilities as a Component of the National Security

DOI: https://doi.org/10.46398/cuestpol.3971.48

Andrii Ighorovych Denysov *
Hennadii Yevhenovych Bershov **
Viacheslav Vitaliiovych Krykun ***
Olha Zhydovtseva ****

Abstract

The issue of protecting critical infrastructure as one of the components of national security is analyzed. The following methods were used in the study: bibliographic, dialectical, empirical, and theoretical, comparative, and legal. The essence of the term «critical infrastructure" is explained both according to the opinions of scientists and from the very position of the authors of the article. The importance of proper protection and proper functioning of infrastructure in Ukraine is well founded. It emphasizes the fact that for many years the issue of the importance of protecting critical infrastructure has been almost forgotten and is not relevant to the governing bodies of the state. In addition, this situation applies to many other countries in the world. The current situation shows that there are countries that, despite being among the most prosperous and innovative, did not pay attention to their situation with their own security infrastructure. It is concluded that, based on a comparative analysis of international experience, in addition to exploring the peculiarities of national realities, the article proposed measures to improve the internal state of protection of critical infrastructure.

Keywords: critical infrastructure object; national security; infrastructure protection; state security policy; geopolitics of security.

* Candidate of Legal Sciences, Associate Professor of the Department of Legal Support of Economic Activity of the Faculty No. 6, Kharkiv National University of Internal Affairs. ORCID ID: https://orcid.org/0000-0002-6256-0172

** Ph.D. in Law, President Judge of the Second Administrative Court of Appeals. ORCID ID: https://orcid.org/0000-0002-3439-5544

*** Doctor in Law, Associate Professor, Assistant Rector of Kharkiv National University of Internal Affairs. ORCID ID: https://orcid.org/0000-0003-1089-555X

**** Candidate of Law, Associate Professor of the Department of Law Enforcement and Police of the Faculty No. 6, Kharkiv National University of Internal Affairs. ORCID ID: https://orcid.org/0000-0003-4637-8490

Recibido el 21/09/2021 Aceptado el 16/11/2021

Protección de instalaciones de infraestructura crítica como componente de la seguridad nacional

Resumen

Se analiza el tema de la protección de la infraestructura crítica como uno de los componentes de la seguridad nacional. En el estudio se utilizaron los siguientes métodos: bibliográfico, dialéctico, empírico y teórico, comparativo y legal. La esencia del término "infraestructura crítica" se explica tanto de acuerdo con las opiniones de los científicos como desde la propia posición de los autores del artículo. Se fundamenta la importancia de la protección adecuada y el buen funcionamiento de la infraestructura en Ucrania. Se enfatiza el hecho de que durante muchos años el tema de la importancia de la protección de la infraestructura crítica ha sido casi olvidado y no es relevante para los órganos de gobierno del estado. Además, esta situación se aplica a muchos otros países del mundo. La situación actual demuestra que hay países que, a pesar de ser parte de los más prósperos e innovadores, no prestaron atención a su situación con una infraestructura de seguridad propia. Se concluye que, a partir de un análisis comparativo de la experiencia internacional, además de explorar las peculiaridades de las realidades nacionales, el artículo propuso medidas para mejorar el estado interno de protección de la infraestructura crítica.

Palabras clave: objeto de infraestructura crítica; seguridad nacional; protección de infraestructura; política estatal de seguridad; geopolítica de la seguridad.

Introduction

The need to protect important infrastructure is one of the most important priorities of the state. The importance of the safe operation of critical infrastructure, namely its key facilities, is a major factor in ensuring national security, sustainable functioning of the economy, welfare, and protection of the population (Chumachenko, 2017). At the same time, global tendencies to increase the threats of natural and man-made nature, increase in the level of terrorist threats, increase in the number and complexity of cyberattacks have led to the actualization of the issue for protecting systems, facilities and resources that are critically important to society, socio-economic development of the state and ensuring national security (Kraivska, 2021).

It is necessary to state the indisputable fact that the attention to protection and qualitative improvement of infrastructural facilities has been recently increased among the countries of the world. It is especially

true of those infrastructure facilities that are critically valuable (important) to the national security of the state.

It is known that after the "Servant of the People" party and its leader Volodymyr Zelenskyi, who was elected the sixth President of Ukraine, came to power in Ukraine in 2019 as a result of democratic and transparent elections, the infrastructure program "Large Construction" was launched, which was the initiative of the new authorities. This program, as officially stated in its plan, is aimed at carrying out large-scale repair and construction works throughout Ukraine. Roads, bridges and other facilities of national and local infrastructure, which are important for society and the state, are among the highest priorities. In addition, the program intends to create new and improve existing schools, hospitals, and other socially important institutions. The initiators of this state program claim that its implementation can increase the level of economic well-being of the state and its citizens. In particular, it is expected that it will be able to raise the country's GDP due to the fact that the new quality infrastructure, which is expected to be the final result of this program, can increase the intensity of cooperation between various economic subjects in Ukraine and can help to make the country more attractive for foreign tourists and investors. Researchers' views on this program are quite different.

The purpose of this article should be to justify the importance of protecting critical infrastructure facilities at the national and local levels for the security of the state, its citizens and institutions.

The objectives of the article are to search for and carefully analyze methods and ways to protect critical infrastructure facilities, to define specific reasons for the importance of a well-functioning infrastructure for the national security and to reveal the terms of "critical infrastructure", "element of the national security", etc.

1. Methodology

The problems of the importance for protecting and proper functioning of infrastructure facilities, especially those that are critical to ensure national security, has been addressed by many researchers and scholars who studied those problems and issues in various fields of science.

The bibliographic method was used that assisted to received up-to-date information on the current state of affairs in the field of protecting critical infrastructure facilities from the leading foreign and domestic researchers of the present time.

The use of dialectical, empirical and theoretical methods was useful in revealing the terms related to the subject matter of this article.

The comparative and legal methods helped to analyze and detail the existing methods of protecting infrastructure facilities that are critically important for the national security of the state, as well as their compliance with domestic, socio-political realities were studied. This method was also used in the analysis of the current state of affairs in the field of protecting infrastructure facilities in the developed world countries. Particular attention was paid to those states that were progressive in accordance with international standards in regard to the issue studied in this article.

2. Results of the Research and Discussion

The rapid growth of information technology has triggered the redistribution of real power in society from traditional structures to information flow control centers. Information technology is finding ever-widening applications in such areas as financial circulation and securities market, communications, transport, high-tech industries (especially nuclear, chemical, etc.), government management systems, etc. Today, the dissatisfaction with the state of Ukrainian information legislation and the need for urgent measures to improve it are obvious.

However, there is no unity in the ways of qualitative transformation of information legislation of Ukraine among researchers of this issue, which is logical, given the complexity, dynamics, and scale of modern information processes that occur in the formation of the national legal system (Politanskyi, Lukianov, Ponomarova, Gyliaka, 2021). Can confidently state that an efficient and smoothly functioning infrastructure in today's world is one of the key elements of the well-being of the state and its citizens. After all, strong and wide bridges, level roads and other facilities of "communication" infrastructure allow people and goods to move quickly in space between different regions of the country (Critical Infrastructure Protection, 2020).

Thus, they provide an opportunity to increase the interaction between different individuals and legal entities (including enterprises) representing different regions of the state. At the same time, besides critical infrastructure communication facilities, it is noted that the main part of the category "critical infrastructure facilities" consists of enterprises and institutions, whose operation is "strategically important for the existence of the state" and for the inviolability of the national security. For example, according to the list of critical infrastructure facilities approved by the Resolution of the Cabinet of Ministers of Ukraine "On approval of the Procedure for forming a list of information and telecommunication systems of critical infrastructure facilities of the state" dated from August 23, 2016, No. 563 this list regardless of ownership includes enterprises, institutions and

agencies representing such industries as: energy, transportation, chemical industry, information technology, food, finance, telecommunications, utilities, health care, banking (The National Infrastructure Protection Plan, 2006).

It is common to distinguish enterprises related to the production or storage of electricity, oil, gas, large water tanks and reservoirs, hydroelectric power plants, etc. among the institutions classified in the energy sector. It is also known that not every institution in the banking and financial sector is recognized as critically important to the national security of the state. It is argued that the critical infrastructure institutions in this area include those, whose sustainable operation "is essential for the economy and security of the state, the existence of society and those that are of significant public interest" (Osypchuk, 2020: 34). This list includes all banks recognized by the National Bank of Ukraine as systemically important. At the same time, all banking institutions that are in the status of critical infrastructure facilities and are 100% of the list of systemically important, that is, both lists duplicate each other.

The approaches to determining the content of such a category as "threats to national security" are changed with the development of the concept of "critical infrastructure". This should be reflected in administrative activities of the Security Service of Ukraine and should be enshrined in the relevant regulatory acts and create a solid foundation for the protection and security of critical infrastructure of Ukraine (Osypchuk, 2020).

On the basis of generalization and analysis of the current legislation in the field of national security and defense, O. V. Nesterenko (2020) has defined the system of subjects of national security and defense of Ukraine as follows: 1) management subsystem (the President of Ukraine); 2) controlled subsystem: security forces – law enforcement and intelligence agencies, state agencies of special purpose with law enforcement functions, civil defence forces and other agencies; Defense Forces – the Armed Forces of Ukraine, as well as other military formations, law enforcement and intelligence agencies, special purpose agencies with law enforcement functions formed in accordance with the laws of Ukraine; defense-industrial complex; citizens and public associations; 3) auxiliary parts of the system (Verkhovna Rada of Ukraine, Cabinet of Ministers of Ukraine, judicial agencies, international institutions).

In our opinion, some of the achievements of the developed countries in the field of protecting critical infrastructure facilities should become a model for Ukraine. It should be noted that the term of "protection of critical infrastructure facilities" means not only its physical or legal protection from dangers and encroachments, but also constant work on its improvement and bringing it into line with modern standards.

For example, it is applied to regular maintenance and construction works on such facilities to prevent them from losing their effectiveness or functionality. It can also include the introduction of new or revision of existing standards of safety and quality of work, which is especially critical for institutions and enterprises that in their direct activities interact with hazardous substances or transport them (Critical infrastructure protection, 2021).

It is worth noting that according to recently published research conducted by foreign scholars, high technology is one of the most important components of efficiency and reliability of institutions and departments that are part of critical infrastructure facilities.

The seriousness of the "technological issue" in compatible infrastructure industries is growing stronger over the time. Most of the current activities for the protection and proper maintenance of infrastructure facilities are carried out using high-tech devices, as well as software both of domestic and mostly foreign production.

Security experts point out that cyberspace threats are currently the biggest threat to critical infrastructure facilities. Given the high level of "computerization" in today's world, public and private institutions that carry out control and protection of the above-mentioned critical infrastructure facilities are trying to protect themselves as much as possible from real and potential cyber threats.

In order to properly protect cyberspace in a particular country, the following two conditions must be met. First of all, effective executive activities of agencies that carry out protection of critical infrastructure facilities should be ensured (Protection of Critical Infrastructure, 2020).

Secondly, these activities should be supported by qualitative legislation in order to make it more effective. It is noted that despite certain mistakes and negative factors, which currently enrich the realities of the domestic sphere of combating cybercrime, we can say that Ukrainian society and government are taking some positive steps towards creating reliable mechanisms to protect cyberspace, including critical infrastructure facilities.

Thus, considering the legal basis for the functioning of domestic cybersecurity systems, regarding the protection of infrastructure facilities, it is necessary to note the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" (October 5, 2017, No. 2163-VIII). This regulatory legal act, among other things, defines critical infrastructure facilities as "enterprises, institutions and organizations, regardless of ownership, ... of great importance to the economy and industry, the functioning of society and public safety....". This legal act also states that the "decommissioning or malfunctioning" of these facilities "may have a negative impact on the

state of the national security and defense of Ukraine..., may pose a threat to human life and health".

Given the fact that this law has a direct focus on cybersecurity sector, it also specifically defines the term of "critical information infrastructure" as "a set of critical information infrastructure facilities".

Thus, we note that the importance of this law primarily lies in providing a clear definition and relative systematization of subjects, objects and legal phenomena related to ensuring cybersecurity and protection of critical infrastructure facilities. It is recognized important mainly because a legal act (specified Law) appeared in Ukraine for the first time after a long time, which is supported by a real, actively functioning program of the government, the National Bank and other state agencies.

Each of the indicated institutions outlined its activities in this direction by its own statutes and special by-laws. On this basis, we argue that finally we received a balanced comprehensive approach to solving existing problems in the field of critical infrastructure protection by various public authorities (Insuring Public Buildings, Contents, Vehicles, and Equipment Against Disasters, 2020).

Ukraine, having this approach to solve a specific problem, becomes on a par with politically and economically developed countries, such as the United States, Canada, and Western Europe countries. The vast majority of both domestic and foreign researchers strongly support the statement that this way of solving existing problems with infrastructure facilities will bring positive results (Ismael and Aaron, 2020). Other existing problems of the Ukrainian state and society should be solved in a similar way. We fully agree with the views of researchers and scholars regarding this issue and argue that those successes that have been recently achieved should be further developed. To this end, government agencies and departments of Ukraine, which are responsible for the proper protection and operation of critical infrastructure facilities of Ukraine, should follow the example of the developed countries (Understanding and Pursuing Information Advantage, 2020).

In particular, we should pay attention and try to adopt the technological solutions that are used in the United States or European countries to protect infrastructure facilities. It is especially true about their methods and means of protection within cyberspace (OPSWAT, 2019). The Department of Homeland Security, which includes federal agencies and institutions, also operates in the United States as the coordinating agency.

We suggest among the specific propositions for improving the systems and mechanisms for the protection of critical infrastructure facilities to introduce the uniform safety standards at these facilities.

Having studied the problematic issues of further development of the state system of critical infrastructure protection, D. H. Bobro (2017) identified the following areas that do the world's countries: 1. Develop the normative base and regularly review it. 2. Determine the coordinating agency. 3. Develop methodological approaches, form a list of critical infrastructure, assess the threats and risks of critical infrastructure, develop response plans, regularly evaluate their effectiveness (for example, the National Center for Analysis and Simulation of Infrastructure of the Home Affairs Ministry takes care of this issue in the US). 4. Provide training of qualified personnel in the field of critical infrastructure protection. 5. Organize the exchange of information and best practices. 6. Develop public and private partnership.

Detailing and revealing this proposition more deeply, we note that the option of implementing this proposition may be a single (unified) "set" of solutions and specific actions that must be implemented by the management of a critical infrastructure facility in case of the threat of attack, natural disasters, and other emergencies (Cyber Security Strategy, 2016). At the same time, the protection of infrastructural facilities that are critically important for the state does not have to be entrusted to a single institution.

The main thing is that public and private agencies that carry out these security activities adhere to common standards. We also consider it necessary to suggest the introduction of a mechanism to control the selection and further operation of the software, which is the basis for the system of protection of critical infrastructure facilities (The History of Critical Infrastructure Protection, 2021). It is due to the fact that Ukraine must seriously care about the process of selecting and implementing foreign software in its own infrastructure protection system in the context of the ongoing armed and information conflict with the Russian Federation, as well as due to the growing "cyber espionage" by China and other authoritarian states (NISS, 2020).

As an example of the dangerous impact of "hostile" software on operating systems and access to private information, we should note the Russian anti-virus "Kaspersky system", which has been repeatedly noticed and recorded in illegal access to personal information of customers and its subsequent transfer to Russian state military and security agencies.

About China, we emphasize that its illegal interference into cyber systems of critical infrastructure facilities of Western countries is mainly due to industrial espionage. Thus, it concerns the theft of the necessary information to take over the secrets of manufacturing and application of certain technologies (Demos, 2021). Instead, a serious and well-thought-out approach to the processes related to the selection and implementation of the necessary software into the infrastructure protection system will significantly improve the domestic infrastructure protection system (Khazaei and Amini, 2021). We should separately note that these

propositions should contain the best elements of the experience of leading foreign countries in this area and should be adapted to domestic realities (Rehak, 2019).

Conclusions

Summarizing all the theses, statements and scientific views of researchers presented in this article, as well as forming the author's final conclusions based on them, we note that the protection of critical infrastructure facilities is one of the key elements for functioning of the state's national security.

Achieving a proper (effective) state of affairs in the field of protecting critical infrastructure facilities will be possible only if there is successful implementation of several components listed and detailed in this article.

First of all, it concerns the creation and smooth functioning of clear legislative and legal regulation, which should facilitate to make the state policy on the protection of critical infrastructure facilities clear and unambiguous.

Secondly, it is noted that the development and improvement of the system of protecting infrastructure facilities must be accompanied by the mandatory use of high technology in the activities of the competent authorities for the protection of critical infrastructure.

The emphasis is placed on the fact that the level of "processibility" or scientific and technical provision of a particular state is currently a major factor in its ability to reliably protect its own critical infrastructure.

This logically implies the conclusion about the importance of a reliable cybersecurity system at enterprises, institutions, and other facilities, which are included in the list of critical infrastructure facilities according to the legislation of the country.

In particular, the author has made own suggestions that the cybersecurity system at the above facilities should be based on uniform standards (rules) of operation. The importance of fruitful interaction of domestic structures involved in this sphere with developed countries has been especially emphasized.

Bibliographic References

BOBRO, Dmytro. 2017. Improvement of the methodology for ranking critical infrastructure facilities and their classification as critical infrastructure. Available online. In: http://old2.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf. Consultation date: 10/05/2021.

CHUMACHENKO, Serhii. 2017. "Natural-technogenic threat assessment for critical infrastructures objects" In: Scientific bulletin: Civil protection and fire safety. Vol. 1, No. 3, pp. 41-47.

CRITICAL INFRASTRUCTURE PROTECTION. 2020. Force point Security Report. Available online. In: https://www.forcepoint.com/es/cyber-edu/critical-infrastructure-protection-cip. Consultation date: 05/05/2021.

CRITICAL INFRASTRUCTURE PROTECTION. 2021. The European Commission's science and knowledge service. Brussels. Available online. In: https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection. Consultation date: 08/05/2021.

CYBER SECURITY STRATEGY. 2016. Federal Office of Civil Protection and Disaster Assistance (BBK). Available online. In: https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1. Consultation date: 08/05/2021.

DEMOS, Jeffrey. 2021. What is Critical Infrastructure Protection and why is it Important. Available online. In: https://firebarrierexperts.com/what-is-critical-infrastructure-protection-and-why-is-it-important/. Consultation date: 15/05/2021.

INSURING PUBLIC BUILDINGS, CONTENTS, VEHICLES, AND EQUIPMENT AGAINST DISASTERS. 2020. RAND Report. Available online. In: https://www.rand.org/pubs/research_reports/RRA332-1.html. Consultation date: 15/05/2021.

ISMAEL, Arciniegas Rueda; AARON, Clark-Ginsberg. 2020. The Downside of a Lean Electric Grid. Commentary (The Hill). Available online. In: https://www.rand.org/blog/2020/10/the-downside-of-a-lean-electric-grid.html. Consultation date: 11/05/2021.

KHAZAEI, Javad; AMINI, Hadi. 2021. "Protection of large-scale smart grids Against false data injection cyber-attacks leading to blackouts" In: International Journal of Critical Infrastructure Protection. Vol. 35, No, 02, pp. 14-23.

KRAIVSKA, Inna. 2021. Monitoring of economic security of enterprises and institutions of social infrastructure in system of national security of the state. A thesis on the degree of Candidate of Economic Sciences in Specialty. O.M. Beketov National University of Urban Economy in Kharkiv. Kharkiv, Ukraine.

LAW OF UKRAINE. 2017. On the Basic Principles of Cybersecurity in Ukraine No. 2163-VIII. October 5, 2017. Available online. In: https://zakon.rada.gov.ua/laws/show/2163-19#Text. Consultation date: 05/08/2021.

NESTERENKO, Alexander. 2020. "System of subjects ensuring national security and defence of Ukraine" In: Law and Safety. Vol. 77, No. 2, pp. 33-39.

NISS. 2020. The State Critical Infrastructure Protection System in the National Security System: The Analytical Report. Kyiv. Available online. In: https://niss.gov.ua/sites/default/files/2020-12/english-version-cip-dopovid_0.pdf. Consultation date: 07/05/2021.

OPSWAT Unveils New Critical Infrastructure Protection Cybersecurity Training and Certification Program. 2019. Available online. In: https://www.prweb.com/releases/opswat_unveils_new_critical_infrastructure_protection_cybersecurity_training_and_certification_program/prweb16603989.htm. Consultation date: 07/05/2021.

OSYPCHUK, Ivan. 2020. "Administrative Activity of the Security Service of Ukraine as the Basis for Ensuring Critical Infrastructure" In: Law and Safety. Vol. 78, No. 3, pp. 32-37.

POLITANSKYI, Viacheslav; LUKIANOV, Dmytro; PONOMAROVA, Hanna; GYLIAKA, Oleh. 2021. "Information Security in E-Government: Legal Aspects" In: Political Questions. Vol. 39, No. 69, pp.361-372.

PROTECTION OF CRITICAL INFRASTRUCTURE. 2020. Cybersecurity and Infrastructure Security Agency (CISA). Available online. In: https://www.cisa.gov/protecting-critical-infrastructure. Consultation date: 07/05/2021.

REHAK, David. 2019. "Complex approach to assessing resilience of critical Infrastructure elements" In: International Journal of Critical Infrastructure Protection. Vol. 25, pp. 125–138.

THE HISTORY OF CRITICAL INFRASTRUCTURE PROTECTION. 2021. Available online. In: https://www.fortinet.com/resources/cyberglossary/critical-infrastructure-protection. Consultation date: 05/05/2021.

THE NATIONAL INFRASTRUCTURE PROTECTION PLAN. 2006. Available online. In: https://www.dhs.gov/xlibrary/assets/NIPP_Overview.pdf. Consultation date: 05/05/2021.

UNDERSTANDING AND PURSUING INFORMATION ADVANTAGE. 2020. The Cyber Defense Review (pp. 109–123). Available online. In: https://www.rand.org/pubs/external_publications/EP68673.html. Consultation date: 10/05/2021.

UNIVERSIDAD
DEL ZULIA

CUESTIONES POLÍTICAS

Vol.39 Nº 71

Esta revista fue editada en formato digital y publicada en diciembre de 2021, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org