Substantiation of the critical infrastructure essence on the example of foreign countries

Maryna Potetiuieva * A

A JSC «Ukrainian railways», 5, Tverskayast., Kyiv-150, Ukraine

Received: August 10, 2020 | Revised: August 27, 2020 | Accepted: August 31, 2020

JEL Classification: R40

DOI: 10.33445/sds.2020.10.4.14

Abstract

The article deals with the essence of critical infrastructure and criteria for its identification on the example of foreign countries. The main reasons that propelled the study of the critical infrastructure issue have been identified. The category “critical infrastructure” is analyzed on the example of countries that are members of NATO and countries that are not members of NATO, and approaches to identifying critical infrastructure objects are established.

Key words: critical infrastructure, security, protection, foreign countries.

Introduction

The rapid development of technology over the past decades, especially in IT sector, has contributed to a significant and sometimes revolutionary increase in the degree of interconnection, interpenetration and interdependence of various networks and systems, production, financial, trade and other processes in all spheres of life in most countries of the world. This significantly increases vulnerability of such systems and facilities and makes ensuring their reliable protection and security much more difficult. At the same time the above-mentioned developments were taking place against the background of a sharp aggravation of terrorism threats, especially international terrorism, growing number of technological disasters, particularly caused by human error, increasing frequency of natural disasters due to global climate change.

Taking into consideration the huge number of factors that affect the life of modern people, society and the state in one way or another, it is extremely important to clearly outline the range of systems, networks and facilities that provide the population, society and the state with critical services for their existence and perform the necessary functions. This is the task the critical infrastructure needs to fulfil. In peacetime, functioning of critical infrastructure is associated with maintaining vital functions in society, protecting the basic needs of its members, and creating a sense of safety and security in them.

Thus, there are such systems, facilities and resources in the world destruction or disruption of which will have a significant negative impact on citizens, society and state institutions.

Results and discussion

Specialists began to study critical infrastructure issues only at the end of the last century. The events of the mid-90s (a terrorist attack in Oklahoma City in 1995, publishing conclusions of the report of the Defense Science Board on information warfare in 1996) [1], as

* **Corresponding author:** Head of the Office JSC «Ukrainian railways», PhD in Economics, Associate Professor, e-mail: marina11176@ukr.net

well as total computerization of management and control systems of various sectors of critical infrastructure significantly increased the importance and necessity of studying this issue.

In July 1996, the President's Commission on Critical Infrastructure Protection (PCCIP) was formed in accordance with Executive order No. 13010 "On work to investigate the vulnerability of critical infrastructure protection against cybernetic and physical threats" (President's Commission on Critical Infrastructure Protection – PCCIP) [2]. The first report of the Commission was published after a year. Its goal was to test the growing dependence of the American economy and lifestyle on critical infrastructure. In October 1997, the Commission issued a report calling for the safety and security arrangements of the United States and its increasingly vulnerable and interconnected infrastructure, such as telecommunications, banking and finance, transportation, and essential public services.

In 1998, the PDD-63 (Presidential Decision Directive), known as the "White Paper", was issued, where objects of critical infrastructure in the public and private sectors and their vulnerability were identified. In this Directive, Bill Clinton introduced the term "critical infrastructure" for the first time [3]. This changed the understanding of the importance of the infrastructure as a whole. Moreover, this directive introduced a definition that includes not only tangible but also intangible elements. These include, first of all, information and cyberspace as one block, in which data is created, transmitted and stored. Critical infrastructure also includes telecommunications, energetics, banks, finance, transportation, water supplies, and rescue services.

In the USA Patriot Act (2002), clause 1016 "Critical Infrastructures Protection" critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [4]. At the same time, according to this document, a well – known organization was founded: National Infrastructure Simulation and Analysis Center (NISAC). The task of the center was to "identify sources at the national level to determine the objects subject to protection of critical infrastructure and ensure development by supporting counter-terrorism measures, risk assessment and risk minimization".

The countries of Western Europe are among the first countries that started to explore the issue of identification and protection of critical infrastructure. In 1999, the National Infrastructure Security Coordination Centre was opened in the UK. Its task was to develop and coordinate activities for protection and defense of critical national infrastructure, within which systems that play an important role in ensuring state functioning were identified. Disruptions or failures of such systems could cause harm to life of the population and serious negative economic and social consequences. These systems included the supply of electricity and fuel, water, food, nutriments, transport, and all public services, including healthcare, communications, banking, etc. [5].

Later on, other European states joined the initiative. The solution to critical infrastructure problems was significantly affected by the terrorist attacks of September 11, 2001 in the United States, March 11, 2004 in Madrid, and later, July 7, 2005 in London underground.

As a result of these terrorist attacks, discussions on security in the European Union have begun. In 2002 the North Atlantic Alliance, within the framework of the Euro-Atlantic Partnership Council, has determined that "critical infrastructure includes physical and cyber systems to support important and necessary economic and public administration activities". It includes, first of all, telecommunications, energy, banking, financial systems, water supply systems and emergency services, both public and private.

In October 2004, the first concept of integrated critical infrastructure and its protection and defense was developed: "Protection of critical infrastructure in the fight against terrorism" [6], which proposed measures for training and response capacity at the European level to terrorist acts aimed at critical infrastructure. Critical infrastructure is defined as "equipment, services, and information systems so vital that their incapacity or destruction will weaken the national society, national economy, public health, security, and effective operation of the state system".

On 17th November 2005 the Commission adopted the "Green Paper on a European Programme for Critical Infrastructure Protection" (EPCIP) [7]. This strategic document focuses on the political and professional spheres in order to include a large number of subjects and obtain specific information from them for shaping the policy of the European critical infrastructure. According to the document, effective protection of critical infrastructure requires interconnection, coordination and cooperation at both national and European levels between all stakeholders – infrastructure owners and users, regulatory authorities, professional organizations and industry associations, as well as at all levels of state and public administration and the public. Special attention is paid to cases where a risk of a domino effect exists (cascading events that are generated by each other).

In Council Directive 2008/114 / EC of 8 December 2008, critical infrastructure is classified into national and European [8, P. 75-80]. The national critical infrastructure includes "means, systems and their parts located in an EU member state that are so essential for the preservation of the most important public functions, health, safety, ensuring normal economic or social conditions for the population, that their incapacity or destruction would have significant consequences for the member states as a result of the disruption of such functions". It is commonly known that some elements of infrastructure can be of great importance not only at the national level, but also at the international level, so the category "European critical infrastructure" is also defined, and it includes "critical infrastructure located in member countries, incapacity or destruction of which would cause significant consequences for at least two states. This also applies to the consequences caused by intersectoral dependence on other types of infrastructure" [9].

The Directive focuses on the energy and transport sectors, moreover, in assessing their impact, it is necessary to add other sectors to its scope of application, namely the information and communication technology sector. Within the Community, the incapacity or destruction of a certain number of critical infrastructures can cause significant cross-border consequences.

In 2016, the European Union adopted another Directive on the protection of critical information infrastructure, namely Directive No. 2016/1148 of the European Parliament and the Council of the European Union "Concerning measures for a high common level of security of network and information systems across the Union" dated 06.07.2016 [10].

Analysis of the definition of the term "critical infrastructure" on the example of foreign countries

A different list of vital (critical) infrastructures (objects) is defined in the legislation of European countries in the field of critical infrastructure protection. It is determined in accordance with the traditions, social and political beliefs, as well as the geographical and historical characteristics of each state.

In Austria, the term critical infrastructure refers to natural resources, services, information technology, networks, and other assets that, if disrupted or destroyed, can significantly affect the health, safety, economic well-being of citizens or the effective functioning of government [11].

In the Netherlands, critical infrastructure includes products, services, and related processes (software, hardware, and data) that, if disrupted or incapacitated, can cause serious social problems – huge casualties or serious economic losses [12].

The critical infrastructure of Germany means the structures and systems necessary to maintain the most important functions of society, the constant availability of which guarantees each member of society a sense of their own and public safety [13].

Switzerland has determined that critical infrastructure is such infrastructure disruption, failure, or destruction of which can significantly affect public health, public affairs, the environment, security, and socio-economic well-being [14].

Critical infrastructure in the Czech Republic includes such systems and services non-functionality of which will have a serious impact on the state security, its economy, public administration, and the provision of basic daily needs of the population [15].

Non-NATO countries also pay attention to the issue of critical infrastructure.

Thus, in the Russian Federation, the term "critically important objects of infrastructure" is used; it refers to such objects incapacity (or termination of functioning) of which can lead to disruption of management, destruction of infrastructure, irreversible negative changes (or destruction) of the economy of the country, subject or administrative-territorial unit, or to a significant deterioration in the safety of life of the population living in these territories for a long time [16].

With regard to the Republic of Belarus, in accordance with paragraph 2 of the Regulation on classifying informatization objects as critical and ensuring the security of critical informatization objects, approved by the Decree of the President of the Republic of Belarus on 25.10.2011 No. 486 "On certain measures to ensure the security of critical informatization objects", critical informatization objects include the objects disruption of the regular operation mode of which can lead to an emergency of a technogenic nature, as well as to significant negative consequences for national security in political, economic, social, information, environmental and other spheres [17].

It should be noted that the definitions of this term in the legislation of leading countries and international organizations are approximately the same, but there are also certain differences that obviously reflect the national or organizational specifics of the scope of the term, the features of their regulatory systems [18].

Critical infrastructure of Ukraine means such systems and resources, physical or virtual, that provide functions and services, the disruption of which can lead to the most serious negative consequences for the life of society, socio-economic development of the country, and national security [18, p. 11].

Conclusions

Currently, in legislation of some countries the definition of "critical infrastructure" has already shifted somewhat from the physical dimension of critical systems, facilities and resources to the functions and services they provide. It is the functions and services that these critical infrastructure facilities and systems provide to society, business and the state that are the basis for determining their criticality, which provides effective methodological opportunities for determining the criteria for selecting critical infrastructure elements and prioritizing their protection.

Summing up the above mentioned and taking into account the experience of foreign countries in ensuring defense capability based on the concept of critical infrastructure, the category "critical infrastructure" can be defined as follows: critical infrastructure means services in certain spheres (energy, transport, banking, financial market, health, drinking water supply, digital infrastructure) that are vital in terms of maintaining social and/or economic activities; critical infrastructure depends on network and information systems; a possible incident regarding them may have a significant negative impact on the level of defense capability and national security of the state. Further research will determine the main approaches to identifying critical infrastructure in the context of countries that are members of NATO and non-members of NATO.

References

1. Fast Analysis Infrastructure Tool Department of Homeland Security's Information Analysis and Infrastructure Protection. National Infrastructure Simulation and Analysis Center (NISAC). URL: https://www.osti.gov/servlets/purl/1413640 (accessed 11.04.2019).

2. Executive Order. 13010. Critical Infrastructure Protection. *Federal Register*. 1996. Vol. 61. №. 138. July 17. P. 3747-3750.
3. Presidential Decision Directive 63. Protecting America’s critical infrastructures. URL : https://fas.org/irp/offdocs/pdd-63.htm (accessed 11.04.2019).
4. Public law 107–56 oct. 26, 2001. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT) Act of 2001. URL: https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf (accessed 11.04.2019).
5. Kovařík J. Kritická infrastruktura a ochrana obyvatelstva, In: Ochrana obyvatel, 2007, Ochrana kritické infrastruktury. S. 145-153.
6. Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the fight against terrorism. Commission of The European Communities, Brussels 20.10.2004.
7. Green Paper on a European Programme for Critical Infrastructure Protection: European Commission, 2006. URL : https://eur-lex.europa.eu/legal-content/en/TXT/?uri= CELEX:52005DC0576 (accessed 11.04.2019).
8. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. *Official Journal of the European Union*, 2008. P. 345.
9. Smetana M. Protection of critical infrastructure. Approaches of the European Union states to determination of critical infrastructure elements. HSB. Technical University of Ostrava, 2014/15.
10. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL : https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed 18.06.2019).
11. Legislative Framework for CIP in Austria. URL: https://cipworkshop.events/wp-content/uploads/2017/10/S4-T2-Legislative_Framework_for_CIP_in_Austria.pdf (accessed 18.06.2019)
12. The policy letter Protecting Critical Infrastructure. URL : https://english.nctv.nl/binaries/20150409-national-security-progress-letter-national-safety-2015_tcm32-84272. pdf (accessed 18.06.2019).
13. National Strategy for Critical Infrastructure Protection (CIP Strategy). URL: http://ccpic.mai.gov.ro/docs/Germania_cip_stategy.pdf (accessed 18.06.2019).
14. National strategy for the protection of Switzerland against cyber risks. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncssmap/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf (accessed 18.06.2019).
15. Regulation No. 317/2014 Coll. on the Determination of Important Information Systems and their Determination Criteria.
16. Critical infrastructure in Russia. TADVISER. URL: http://www.tadviser.ru/index.php. (accessed 13.08.2020).
17. On some measures to ensure the security of critically important informatization facilities: Decree of the President of the Republic of Belarus No. 486 of October 25, 2011. URL : http://base.spinform.ru/show_doc.fwx?rgn= 47499 (accessed 10.11.2019).
18. Green book on the protection of critical infrastructure in Ukraine: collection of materials of international expert meetings / comp.: D. S. Biryukov, S. I. Kondratov; gen. ed. O. M. Sukhodolia. Kyiv: NISS, 2015. 176 p.