

THE ATTITUDE TOWARDS THE CRITICAL INFRASTRUCTURE IN THE REPUBLIC OF SERBIA

*Branislav Milosavljević**, *Dragan Vučinić***

Достављен: 15. 07. 2021.

Језик рада: Енглески

Кориговано: 22. 09. и 08. 10. 2021.

Тип рада: Прегледни рад

Прихваћен: 21. 10. 2021.

DOI број: 10.5937/vojdela2104131M

National policies, strategies, doctrines and laws have a different approach to the issue of critical infrastructure. The adequately designed infrastructure is the main driving force of national prosperity and a precondition for economic expansion and future growth. On the other hand, everyday life in modern times is based, among other things, on highly developed infrastructure, especially in the fields of management and control of energy supply, provision of drinking water sources, transport, maintenance of information technology systems, telecommunications, etc.

The paper considers the issue of critical infrastructure protection on the example of the Republic of Serbia. In this regard, critical infrastructure will be considered through changes in the strategic and normative framework. Historically, the subject area has long been directly related to the defence needs of the state. This is partly expected having in mind that the phrase critical infrastructure is taken from military terminology to denote everything necessary for the functioning of military system during military conflicts, when resources are directed to the preservation of one's own facilities, systems and networks, and also their disabling on the enemy side. However, in modern times, critical infrastructure has gained much broader meaning and significance for the functioning of the state and society as a whole.

Key words: social self-protection, critical infrastructure, infrastructure sectors, national security, defence system

* Strategic Research Institute, University of Defence in Belgrade, Republic of Serbia, branslav.milosavljevic@mod.gov.rs

** Modern Business School, Belgrade, Republic of Serbia

Introduction

The modern concept of critical infrastructure is characterized by a changed perception of threats and increased interdependence between various infrastructural elements. This has influenced critical infrastructure to take on increasing scope, content and complexity, and potential threats and dangers are of paramount importance to national security. The concept of critical infrastructure includes facilities such as buildings, roads and transport, telecommunications, water and energy systems, emergency services, banking and financial institutions and sources of supply, as well as virtual space (cyberspace). In general, critical infrastructure consists of various systems that are necessary for the smooth functioning of power at all levels.¹

Primarily due to the wide scope that also includes the diversity of content, which is multidisciplinary in its nature, defining the term critical infrastructure is a complex process. The term „infrastructure“ can be defined as „the main framework of a system or organization“, while the phrase „critical infrastructure“ can be defined in many ways, having in mind that the term „critical“ is variable and difficult to determine. Artificial networks and systems that provide the necessary services to a wide range of population also contribute to the complexity problem².

Despite the obvious complexity, the term critical infrastructure is usually defined in one of two ways. The first way include all vital infrastructures, as it was the case in the 2003 US C Infrastructure Protection Strategy, as one of the first documents of this kind.³

The second way is based on determining the specificity of system characteristics and their relation to other systems or units, as it is the case with the German National Strategy for the Protection of Critical Infrastructure, which determines criticality as a result of disruption or failure of the supply function and service to the society. From a scientific point of view, the approach that defines criticality as a result of specific characteristics is particularly important. In this case, certain relational characteristics of a system are determined because the given system is critical in relation to other systems or wholes. Namely, the system is critical for the other system when the first is necessary in order to continue the work of the other one. Thus, the German National Strategy for the Protection of Critical Infrastructure defines criticality as a relative measure for the consequences of disruption or failure of a function related to the delivery of goods and services to the society.⁴

¹ Pesch-Cronin A. Kelley, Marion E. Nancy, *Critical infrastructure protection, risk management, and resilience: a policy perspective*, Taylor & Francis Group, 2016, p. 4.

² Škero Mirko, Ateljević Vladimir, *Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa direktivom Saveta Evrope*, *Vojno delo br. 2*, MC „Obrana“, Beograd, 2015, pp. 192-193.

³ The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003.

⁴ Bundesministerium des Innern, *Bundesministerium des Innern Nationale Strategie zum Schutz Kritischer Infrastrukturen*. Berlin, 2009, p. 7.

Etymologically, the root of the term criticality is found in the Greek term *κρίσις* (crisis), which was initially used in medicine to describe a certain condition during an illness in which the patient's fate is determined. When we try to understand the potential of the concept of crisis, it is equally important to study its metaphorical effects. The world crisis and conditions related to the crisis evoke images of radical change, so the term crisis, as such, has become synonymous in modern history with terms such as rebellion, conflict or revolution.⁵ During the early period of the Cold War, the concept of criticality was included in the US Civil Defence Strategy, where it was used in the context of „vulnerability mapping“, as a kind of assessment of the vital parts of the state, that is, important technical infrastructure.⁶

It is also the beginning of the more intensive use of the term in political and other debates to denote and identify organizations and institutions that are in any way important, relevant or necessary for the continuity of supply of goods and services to population and economy. It is common for critical infrastructure to include traffic, transport, energy production and distribution, information and communications systems, health services, water and food supply systems, financial services, state infrastructure, etc. In the circumstances of possible partial or complete failure of these infrastructures, the society and, ultimately, national security are threatened. This is one of the reasons why many countries seek to identify and analyze critical sectors, as well as subsectors, processes and facilities using a variety of methodological approaches. However, the very complexity of infrastructural systems is the greatest common problem of all countries that have approached the identification and development of the critical infrastructure protection policy.⁷

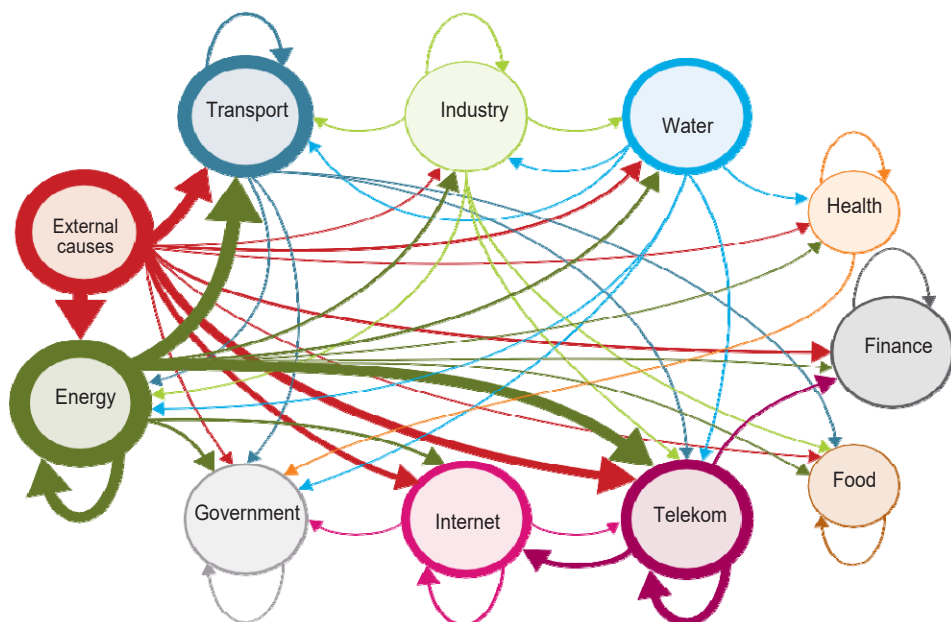
In addition to the mentioned, it should be pointed out that the terms critical infrastructure and critical information infrastructure, which are different, but related terms, are often used in parallel. In this regard, critical infrastructure includes critical information infrastructure, as its part. On the other hand, the consequence of the non-functioning of information infrastructure may be the interruption of the functioning of the overall critical infrastructure. However, critical infrastructure can be threatened for a number of other reasons not related to information infrastructure.⁸

⁵ Reinhart Koselleck et al.: *Geschichtliche Grundbegriffe. Historisches Lexikon zur politisch-sozialen Sprache in Deutschland (Vol. 3)*, Klett-Cotta, Stuttgart, 1982, p. 619.

⁶ Collier J. Stephen, Lakoff Andrew, Distributed Preparedness: The Spatial Logic of Domestic Security in the United States. In: *Environment and Planning D: Society and Space*, 26 (1), 2008, pp. 12-16.

⁷ Lewis, G. Ted, *Infrastructure Protection in Homeland Security, Defending a Networked Nation*, Wiley Interscience, 2006, p. 32.

⁸ Zaballos G. Antonio, Jeun Inkyung, *Best Practices for Critical Information Infrastructure Protection (CIIP), Experiences from Latin America and the Caribbean and Selected Countries*, Inter-American Development Bank, Washington DC, 2016, pp. 3-4.



An example of the relation between critical infrastructure and the cascading effect of dependence disruption⁹

The development of the critical infrastructure protection in the Republic of Serbia

In the former SFRY, in the mid-1950s, the national critical infrastructure encompassed all „state-owned companies“ and was protected by internal security, with the assistance of the police, security and intelligence services. Since the second half of the 1970s, critical infrastructure and all other state or public property in the former Yugoslavia were protected by a comprehensive network, known as the system of social self-protection. In addition to internal security service, this system provided two additional levels of the protection of the company's assets: internal financial control and control of associated workers. Despite the fact that there were three levels of protection (control), theft, damage and other losses and threats to property were still present.¹⁰

⁹ Luijff Eric, et al, *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers*, TNO, Netherlands, 2016, p. 26.

¹⁰ Davidović Dragomir, Kešetović Želimir, Pavičević Olivera, National Critical Infrastructure Protection in Serbia: The Role of Private Security, *Journal of Physical Security* 6(1), 2012, [http://rbsecurty.com/JPS%20Archives/JPS%206\(1\).pdf](http://rbsecurty.com/JPS%20Archives/JPS%206(1).pdf), 24/05/2021, p. 60.

This was followed by the period (1973-1990) in which the concept of social self-protection was implemented, which had its normative framework in two laws,¹¹ and which regulated the organization, as well as the rights and duties of the protection service in companies. All companies were supposed to have an organized protection service, while other organizations and communities had the obligation to organize physical and technical security of facilities. Social self-protection was aimed at direct protection of social property from illegal appropriation and damage to buildings and property, negligent performance of functions and business, violation of business ethics, good business practices, as well as from unfair competition, bribery and corruption, hostile activities and influence, violation of internal order and natural disasters. In that period, the security system referred to physical and technical protection and was the legal basis for companies to adopt a general act for the specific regulation of physical and technical protection of buildings and property.¹²

The Law on the Fundamentals of Social Self-Protection represented the legal and political framework for organizing and implementing social protection of property in companies, activities of local community and every citizen as a subject of public security, relations between public security bodies (the police) and self-protection in companies, as well as conditions for performing the service of direct physical security. Social self-protection took place through three levels:

- internal professional control,
- self-governing workers' control and
- physical, technical and fire security.

The enactment of the Law on the System of Social Self-Protection in 1986 regulated the scope of work of the security service of the organization of associated labour and its place in the security system, such as: main tasks of the service, rights of security workers, their tasks and obligations, use of firearms and other means of coercion used by security workers, selection of personnel, etc. Moreover, the Law, inter alia, provided for the mandatory police check of the existence of a criminal record and the check of psycho-physical capabilities of security service workers.

In addition, the legislator defined that during implementation of physical and technical security measures, the services of organizations registered to perform physical and technical protection of facilities and assets are used, as well as that two or more organizations, i.e. bodies, can jointly organize physical protection of facilities and assets. The Law stipulated that special measures of physical and technical security should be taken in economic systems in order to:

- store and secure facilities, plants and other property,
- detect and prevent actions that may threaten the safety of people and property,

¹¹ The Law on the Fundamentals of Social Self-Protection was in force until 1986 and the Law on the System of Social Self-Protection, Official Gazette of the SFRY.

¹² Nikač Željko, Pavlović Gojko, *Pravo privatne bezbednosti*, Kriminalističko-policijska akademija, Beograd, 2012, pp. 93-96.

- prevent unauthorized persons to access facilities and other premises, and
- implement other measures that provide uninterrupted performance of work.¹³

The Law also provided for the establishment of specialized agencies for the security of persons and property, which was the basis that enabled the establishment of private security agencies in the early 1990s. During the existence of the Federal Republic of Yugoslavia, the Government passed the Decision on defining great technical systems of interest for the country's defence. They are defined as great technical systems of interest for the country's defence and technical resources important for the functioning of these systems. These were the fields of communications, informatics, air and railway traffic, power engineering, water supply, etc. On the other hand, there was an obligation that during selection, construction and development, as well as procurement of technical resources for their functioning, investors harmonize them with the country's defence needs. The mentioned Decision also stipulates the procedure of informing about selection, construction and development of these systems, procurement of technical resources and setting requirements for their harmonization with the country's defence needs.¹⁴

After that, in 1992, the Decree on facilities and regions of special importance for the defence of the Republic of Serbia came into force. In accordance with this Decree, facilities of special importance for the defence of the Republic of Serbia are those which the assessment determines that their damage, i.e. revealing their type, purpose or location, when kept secret, could have serious consequences for the defence and security of the Republic. In other words, this group included facilities and regions in the field of transport, telecommunications and communications, energy, water management and industry. However, this document does not mention terrorism as a security risk, challenge or threat, but it mentions great technical systems, facilities and regions as key facilities "that may be threatened, that have special significance from the aspect of the country's defence and whose threat would endanger the continuity of the state and society functioning".¹⁵

The Decision on defining great technical systems of importance for defence, which was passed in 2009, and updated in 2014 and later, deserves special attention, as an obligation arising from the Law on Defence.¹⁶ In such a way, eight great technical systems in the field of transport and telecommunications, three public companies and four corporations in the field of energy, a public company and a company in the field of coal production, as well as twelve public companies and institutions in the field of water supply, energy transfer, forest management and broadcasting were included in the resources of the critical infrastructure

¹³ The Law on the System of Social Self-Protection, "Official Gazette of SRS" no. 14/86; Bošković Mičo, Keković Zoran, *Obezbeđenje lica, imovine i poslovanja preduzeća*, VŠUP, Beograd, 2000, p. 35.

¹⁴ The Decision on defining great technical systems of importance for the country's defence, "Official Gazette of RS", no. 54/94, 58/94, 65/94 and 10/97.

¹⁵ Nikolić Dejan, Kovač Mitar, Mitić Vlada: *Bezbednosna zaštita objekata od posebnog značaja za odbranu*, *Vojno delo br. 7*, MC „Odbrana”, Beograd, 2018, p. 180.

¹⁶ The Law on Defence, "Official Gazette of RS" no. 116/2007, 88/2009, 104/2009, 10/2015 and 36/2018, Art. 68-70.

in Serbia that are important for the country's defence. This Decision is important because it required the procedure of informing about selection, construction and development of these systems, procurement of technical resources and the manner of their provision, as well as setting requirements for their harmonization with the country's defence needs. The investor was obliged to inform the Ministry of Defence and the responsible ministry about selection, construction of vital, i.e. capital facilities and development of technical systems important for the country's defence, i.e. about the procurement of technical resources of special importance for the functioning of those systems. Along with notification, the investor also enclosed the appropriate investment and technical documentation on a system, i.e. specification for the procurement of technical resources and the explained programme for the development of such a system.¹⁷

In this retrospective of the strategic framework, the Law on Emergency Situations from 2009 is also important, which provides for the competence of the Ministry of Interior for conducting an assessment of the threat from natural disasters and other accidents and submitting it to the Government for adoption. On the other hand, it is defined that provinces, as well as local government units, ministries and other bodies and organizations will do threat assessment in accordance with the scope and submit it to the Ministry of Interior. In addition, the Law stipulates that through threat assessment, the sources of potential endangerment, possible consequences and, accordingly, adequate possibilities for the implementation of measures and tasks on protection and rescue are identified. The assessment included in particular:

- characteristics of a territory, critical facilities, critical places and areas from the point of view of the threat from natural disasters and other accidents, with possible transboundary effects of accidents;
- vulnerability of a territory to natural and other disasters;
- analysis of possible consequences of natural and other disasters; and
- needs and possibilities for protection of people, material goods and environment from the consequences of natural and other disasters.¹⁸

In addition to the above-mentioned, this Law provided for the obligation to draft a Decree on the content and manner of drafting a protection and rescue plan in emergency situations, which was adopted by the Government in 2011. The Decree stipulates that a part of an assessment will be the assessment of critical infrastructure from the point of view of natural disasters and other accidents. At that time, the concept of critical infrastructure was introduced for the first time in the Republic of Serbia. However, there was a lack of a clear definition of elements or fields of infrastructure, as well as entities, that would have the responsibility to protect critical infrastructure. These shortcomings were partially addressed by the new Decree in which ten critical infrastructure sectors can be identified.¹⁹

¹⁷ The Decision on defining great technical systems of importance for defence, "Official Gazette of RS" no. 54/2010, 4/2011, 41/2014, 35/2015 and other.

¹⁸ The Law on Emergency Situations, "Official Gazette of RS" no. 111/2009, 92/2011 and 93/2012, Art. 46.

¹⁹ The Decree on the content and manner of drafting a protection and rescue plan in emergency situations, "Official Gazette of RS" no. 102/2020, Art. 4.

Following the termination of the Law on Emergency Situations, a new legislative framework came into force which, inter alia, defines “disaster risk reduction, prevention and strengthening of resilience and readiness of individuals and communities to respond to disasters, protection and rescue of people, material, cultural and other goods, rights and obligations of citizens, associations, legal entities, bodies of local government units, autonomous provinces and the Republic of Serbia, emergency management, the functioning of civil protection, early warning, notifications and alerts, international cooperation, inspection and other issues of importance for the organization and functioning of the system of disaster risk reduction and emergency management”.²⁰ Analyzing the provisions of this Law, it is obvious that the legislator missed the opportunity to emphasize critical infrastructure with regard to its importance, the interconnection of critical infrastructure sectors and the risk of possible endangerment. The paradoxical situation in this segment is particularly indicated by the Methodology of development and content of disaster risk assessment and protection and rescue plan²¹ – the document of lower generality in which special attention is paid to critical infrastructure. In addition to defining the concept of critical infrastructure, the contents of critical infrastructure sectors are also mentioned, which is particularly important for a more complete understanding. On the other hand, critical infrastructure is considered throughout risk assessment process and, inter alia, as a mandatory scenario content and protected value.²²

Strategic framework for critical infrastructure protection

Within the previous National Security Strategy of the Republic of Serbia from 2009, the term critical infrastructure is not directly mentioned, but can be found indirectly in segments related to problems of the economic development of the Republic of Serbia due to long-term economic sanctions and destruction of vital facilities of economic and transport infrastructure, energy interdependence and sensitivity of infrastructure for production and transport of energy, and high-tech crime and endangerment of information and telecommunication systems.²³

This is also the case in the current National Security Strategy from December 2019, in which the term critical infrastructure is not mentioned at all. On the other hand, there are some indirect references in the part of the Strategy, which say that “different types of natural disasters (floods, droughts, fires, earthquakes, extremely high temperatures, etc.), as well as the presence of large quantities of hazardous

²⁰ The Law on disaster risk reduction and emergency management, “*Official Gazette of RS*” no. 87/2018, Art.1.

²¹ The Methodology of development and content of disaster risk assessment and protection and rescue plan, “*Official Gazette of RS*” no. 87/2018, part A, item 2.

²² *Ibid.*, part B, item 2 and 3.2.

²³ The National Security Strategy of the Republic of Serbia, “*Official Gazette of RS*” no. 88/2009, item II.

substances in production, storage, traffic and transport, directly and indirectly affect the level of risk and safety of people, animals, material and cultural goods and the environment”, as well as that “significant risk is posed by technical and technological accidents, whose consequences can manifest not only in the Republic of Serbia, but also in the territories of neighbouring countries”. The same section of such document states that “the development of modern technology and their presence in all spheres of the society results in an increase in high-tech crime and endangerment of information and communications systems”.²⁴

Instead of protecting critical infrastructure, the Strategy mentions “monitoring, assessing, planning and taking measures to mitigate the effects of climate changes”, “flood and fire protection”, “improving the environment quality”, “efficient management of hazardous waste” and “improving capabilities and capacities for resource management, according to the strategic commitment of the Republic of Serbia for the implementation of internationally accepted standards in the field of protection and improvement of the environmental quality”.²⁵

On the other hand, there are noticeable examples of many countries, including those in the region, which have unequivocally expressed the importance of critical infrastructure in their strategic framework. Thus, for example, the Republic of Croatia has defined “achieving the highest level of security and protection of population, as well as critical infrastructures” as its strategic goal. In addition, the Strategy emphasizes that “safe society requires the protection of life, the rescue of people and goods, as well as the protection of critical infrastructures”.²⁶ A somewhat similar definition can be found in the National Security Strategy of Montenegro, which emphasizes “protection of critical infrastructures by encouraging cooperation between state institutions, civil and private sector, in order to strengthen civil readiness to respond to security challenges, risks and threats”, as national security interest.²⁷

The strategic framework in this field includes the Strategy for the Development of the Information Society and Information Security in the Republic of Serbia from 2021 to 2026. Namely, critical information infrastructure is of special importance for the adequate functioning of all other sectors, and its specificity has influenced many countries to develop a special approach to the protection of this segment. In this regard, this Strategy defines certain priority fields within the development of the information society. A special part of the Strategy is dedicated to critical infrastructure with the provisions that “it is necessary to develop and improve protection against attacks by implementing information technology to critical infrastructure systems, which in addition to ICT systems can be other infrastructural systems that are mana-

²⁴ The National Security Strategy of the Republic of Serbia, “*Official Gazette of RS*” no. 94/2019, item 2.

²⁵ The National Security Strategy of the Republic of Serbia, “*Official Gazette of RS*” no. 94/2019, sub-item 4.7.

²⁶ See: Strategija nacionalne sigurnosti Republike Hrvatske, “*Narodne novine*” br. 73/2017.

²⁷ Strategija nacionalne bezbjednosti Crne Gore, “*Službeni list Crne Gore*” broj 85/2018, tačka 2.

ged by the use of ICT, such as electricity.” In this regard, it is necessary to further define criteria for determining critical infrastructure from the point of view of information security, criteria for characterizing attacks using information technology on such infrastructure in relation to classic forms of attacks, as well as the protection conditions in this field. In addition, the Strategy emphasizes the importance of infrastructure in this field, defining it as a system of special importance, which is why it is necessary to achieve smooth operation because otherwise it can “have great consequences in the cases involving a large number of users, a large part of a territory or public safety”. This is also the main reason why the Strategy provides for some measures in order to achieve preventive action and reduce the consequences of possible incidents.²⁸

The Act on Critical Infrastructure

At the end of 2018, the Republic of Serbia passed the Act on Critical Infrastructure, for the purpose of normative regulation of this field and as the reflection of the need for harmonization with the European legislation. Namely, in accordance with the documents of the European Union, critical infrastructure has to be defined and listed in all member states, as well as in the countries that aspire to become full members of the EU. In this regard, it should be pointed out that the EU is the driving force of many initiatives and programmes aimed at protecting “the European critical infrastructure”. This was particularly incited by the terrorist attacks in Madrid in 2004 and London in 2005. On the other hand, the concept of critical infrastructure security has arisen due to the fear that negative effects, caused by the interruption or non-functioning of critical infrastructure located in some EU member state, could spread to other member states. This primarily relates to energy networks or gas pipelines, as they are located throughout the EU and have vital nodes and critical assets in different member states.²⁹

According to legal framework, the critical infrastructure in the Republic of Serbia includes “systems, networks, facilities or their parts, whose interruption of functioning or delivery of goods, that is services, may have serious consequences for national security, health and lives of people, property, environment, security of citizens, economic stability, i.e. endanger the functioning of the Republic of Serbia”.³⁰ It is particularly important that the legislator has defined the procedure by which systems, networks, facilities or their parts in a certain sector are defined as critical infrastructure according to the criteria. The ministries responsible for certain fields are in charge of the execution of the critical infrastructure identification procedure in some sector,

²⁸ The Strategy for the Development of the Information Society and Information Security in the Republic of Serbia from 2021 to 2026, “*Official Gazette of RS*” no. 86/2021, item 6.2, special objectives item 3.2.

²⁹ Lazari Alessandro, *European Critical Infrastructure Protection*, Springer, 2014, p. 45.

³⁰ The Act on Critical Infrastructure, “*Official Gazette of RS*”, no. 87/2018, Art. 4.

whereby the criteria for the critical infrastructure identification and the manner of reporting are defined by the Government. In this regard, the identification and definition of the critical infrastructure in Serbia is performed in the sectors of energy, transport, water and food supply, health, finance, telecommunications and information technology, environmental protection and the functioning of state bodies.³¹

In addition to eight listed sectors, critical infrastructure can also be defined in other sectors, at the proposal of the ministry responsible for a particular field, and in accordance with this Act. The final list of the critical infrastructure in Serbia is determined by the Government, at the proposal of the Ministry of Interior. The exception is the critical infrastructure within the competence of the Ministry of Defence and the Serbian Armed Forces, whose use, storage, protection, control and supervision are performed in accordance with the provisions of the Law on Defence and the Law on the Serbian Armed Forces. The Act defines critical infrastructure protection as „a set of activities and measures aimed at ensuring the functioning of critical infrastructure in the event of disruption or destruction, that is, protection in the event of threats and prevention of the consequences of disruption or destruction.“³²

In accordance with the European standards, the Act on Critical Infrastructure introduces the term critical infrastructure operator which is related to “state bodies, bodies of autonomous province, bodies of local government units, public companies, companies or other legal entities that manage systems, networks, facilities or their parts as critical infrastructure”. Critical infrastructure operators are required to develop the Operator Safety Plan for risk management, which defines the operator's safety objectives and measures based on risk analysis, and obtain the consent of the Ministry of Interior for it no later than six months after defining systems, networks, facilities or their parts for critical infrastructure.³³

In addition, critical infrastructure operators must have a liaison officer, as a point of contact between the operator and the Ministry of Interior, who provides continuous control of risks and threats, notifies of changes to critical infrastructure and the evaluation of risks, threats and vulnerability, coordinates the Operator Safety Plan for risk management, performs testing through exercises and other activities defined by the Plan and performs all other tasks related to critical infrastructure. A liaison officer is appointed by the Ministry of Interior, based on the proposal of critical infrastructure operator among the employees, and that person must hold an appropriate licence.³⁴

The Act also defines the status of the European critical infrastructure in the Republic of Serbia, which is determined by the Government on the proposal of the Ministry of Interior and on the basis of requests and consents of the interested EU member states. In addition, the Government has the obligation to inform the EU member states on the definition of the European critical infrastructure in the Republic

³¹ The Act on Critical Infrastructure, “*Official Gazette of RS*”, no. 87/2018, Art. 6.

³² *Ibid*, Article 2. Item 4, Article 7.

³³ *Ibid*, Article 2. Item 5, Article 8.

³⁴ *Ibid*, Article 9.

of Serbia. On the other hand, if it is the critical infrastructure located in an EU member state, and it is important for the Republic of Serbia, the Government proposes to the competent body of such a country to define the European critical infrastructure. In this regard, the legislator has defined that the European critical infrastructure in Serbia is protected like the critical infrastructure of the Republic of Serbia, unless it is specifically stipulated by the EU regulations. In addition, the legislator has envisaged that the Ministry of Interior represents a contact for the exchange of information and coordination of activities related to the European critical infrastructure with other member states and bodies of the European Union and also monitors the implementation of laws and regulations in this field.³⁵

Conclusion

For the Balkan countries, except Greece, national critical infrastructure for decades after World War II represented all companies and institutions that were in the state ownership (energy sector, telecommunications, transport, post office, etc.). In the mid-1950s, these facilities in the Republic of Serbia were protected by internal security, engaging the police, security and intelligence services. Since the second half of the 1970s, critical infrastructure and all other state or public property have been protected by a comprehensive network known as the social self-protection system. In addition to internal security service, the system provided two additional levels of protection for the company's property: internal financial control and control of associated workers. In this regard, it is obvious that the Republic of Serbia has a long history of critical infrastructure protection, which, as in other countries, was directly related to the needs for the functioning of the defence system. At the same time, a frequent change of the concept of protection can be noticed as a part of general modifications of internal security.

Like many countries in the region, the Republic of Serbia has started identification, definition and protection of critical infrastructure. The lack of a normative and adequate organizational framework has resulted in undertaking activities to reach the standards of developed countries in this field. The adoption of laws and adequate strategies has established an appropriate normative framework as a basis for further development of critical infrastructure protection system. In this regard, an approach that includes the acceptance of the European standards is obvious, which is of particular importance in the field of meeting the criteria for the EU membership. On the other hand, vagueness or complete harmonization of the national legislative and strategic framework defining this field is also noticeable. Therefore, it is necessary to pay attention to critical infrastructure in the National Security Strategy, as well as in the legislative framework related to risk reduction and emergency management.

³⁵ Ibid, Art. 14, 16; The provisions of the Law on the European Critical Infrastructure will come into force from the day of the accession of the Republic of Serbia to the European Union.

Literature

[1] Bogdan Grenda, Edyta Ślachcińska, *Terrorist Threats for the Critical Infrastructure of the State, Advances in Economics, Business and Management Research*, volume 31, Atlantis Press, 2017.

[2] Бошковић Мићо, Кековић Зоран, *Обезбеђење лица, имовине и пословања предузећа*, ВШУП, Београд, 2000.

[3] Bundesministerium des Innern, *Bundesministerium des Innern Nationale Strategie zum Schutz Kritischer Infrastrukturen*. Berlin, 2009.

[4] Davidovic Dragomir, Kesetovic Zelimir, Pavicevic Olivera: National Critical Infrastructure Protection in Serbia: The Role of Private Security, *Journal of Physical Security* 6(1), 2012, [http://rbsekurity.com/JPS%20Archives/JPS%206\(1\).pdf](http://rbsekurity.com/JPS%20Archives/JPS%206(1).pdf), 24/05/2021.

[5] Zaballos G. Antonio, Jeun Inkyung, *Best Practices for Critical Information Infrastructure Protection (CIIP), Experiences from Latin America and the Caribbean and Selected Countries*, Inter-American Development Bank, Washington DC, 2016.

[6] Закон о систему друштвене самозаштите, „Службени гласник СРС”, бр. 14/86.

[7] Закон о критичној инфраструктури, „Службени гласник РС”, бр. 87/2018.

[8] Закона о одбрани, „Службени гласник РС”, бр. 116/2007, 88/2009, 88/2009, 104/2009, 10/2015. и 36/2018.

[9] Закон о ванредним ситуацијама, „Службени гласник РС”, бр. 111/2009, 92/2011. и 93/2012.

[10] Закон о смањењу ризика од катастрофа и управљања ванредним ситуацијама, „Службени гласник РС”, бр. 87/2018.

[11] Kristof Lukitsch, Marcel Müller, Chris Stahlhu, Criticality in: Jens Ivo Engels, *Key Concepts for Critical Infrastructure Research*, Wiesbaden, Springer, 2018.

[12] Lazari Alessandro: *European Critical Infrastructure Protection*, Springer, 2014.

[13] Lewis, G. Ted : *Infrastructure Protection in Homeland Security, Defending a Networked Nation*, Wiley Interscience, 2006.

[14] Luijff Eric et al : *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers*, TNO, Netherlands, 2016.

[15] Matthew Jude Egan, Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems, *Journal of Contingencies and Crisis Management*, 15, 2007.

[16] Методологија израде и садржај процене ризика од катастрофа и план заштите и спасавања, „Службени гласник РС”, бр. 87/2018.

[17] Никач Жељко, Павловић Гојко, *Право приватне безбедности*, Криминалистичко-полицијска академија, Београд, 2012.

[18] Nikolić Dejan, Kovač Mitar, Mitić Vlada: *Bezbednosna zaštita objekata od posebnog značaja za odbranu, Vojno delo br.7*, МС „Одбрана”, Београд, 2018.

[19] Одлука о одређивању великих техничких система од интереса за одбрану земље „Службени лист СРЈ”, бр. 54/94, 58/94, 65/94 и 10/97.

[20] Одлуку о одређивању великих техничких система од значаја за одбрану „Службени гласник РС“, бр. 54/2010, 4/2011, 41/2014, 35/2015. и др.

[21] Pesch-Cronin A. Kelley, Marion E. Nancy, *Critical infrastructure protection, risk management, and resilience: a policy perspective*, Taylor & Francis Group, 2016

[22] Reinhart Koselleck et al.: *Geschichtliche Grundbegriffe. Historisches Lexikon zur politisch-sozialen Sprache in Deutschland (Vol. 3)*, Klett-Cotta, Stuttgart, 1982,

[23] Стратегија националне безбедности Републике Србије, „Службени гласник РС“, бр. 88/2009.

[24] Стратегија националне безбедности Републике Србије, „Службени гласник РС“, бр. 94/2019.

[25] Strategija nacionalne sigurnosti Republike Hrvatske, „Narodne novine“, br. 73/2017.

[26] Strategija nacionalne bezbjednosti Crne Gore, „Službeni list Crne Gore“, br. 85/2018.

[27] Стратегија развоја информационог друштва у Републици Србији од 2021. до 2026.године, „Службени гласник РС“, бр. 86/2021.

[28] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003.

[29] Уредба о објектима и рејонима од посебног значаја за одбрану Републике Србије, „Службени гласник РС“, бр. 18/92.

[30] Уредба о садржају и начину израде плана заштите и спасавања у ванредним ситуацијама, „Службени гласник РС“, бр. 102/2020.

[31] Collier J. Stephen, Lakoff Andrew, Distributed Preparedness: The Spatial Logic of Domestic Security in the United States. In: *Environment and Planning D: Society and Space*, 26 (1), 2008.

[32] Škero Mirko, Ateljević Vladimir: *Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa direktivom Saveta Evrope, Vojno delo br.2*, МС „Одбрана“, Београд, 2015.

Summary

The term critical infrastructure is relatively recent, and is used more intensively in the scientific and professional literature after the terrorist attacks in the United States in September 2001. The increased importance of the concept of critical infrastructure protection has occurred, among other things, due to changes in the perception of threats to critical infrastructure and the growing interdependence of different infrastructural elements. In recent decades, there has been an evident increase in the vulnerability of the society to various forms of threats, as well as the phenomenon of failure of certain critical infrastructure systems caused by various reasons. In the past, this vulnerability was mostly related to problems in the functioning of high-risk technology. However, nowadays, critical infrastructure is taking on the increasing scope, content and complexity, and potential threats and risks are seen as issues of the utmost importance for national security. In addition to the ever-present danger of natural disasters and technological accidents, new security challen-

ges at the beginning of this century, and particularly the global threat of international terrorism, have contributed to critical infrastructure protection becoming an indispensable part of national security strategies in almost all countries. Given that facilities, systems, processes and operations in parts of critical infrastructure can be compromised in different ways, they are especially protected at national level. In this regard, the mentioned implies appropriate normative, organizational, safety and technical preconditions for their normal functioning, as well as for the prevention and elimination of natural or man-made threatening actions.

The beginning of the critical infrastructure protection in the Republic of Serbia is the period from the mid-1950s, including the state-owned companies and institutions, which were protected by the engagement of various services. This was followed by the introduction of the system of social self-protection, which, among other things, was aimed at direct protection of social property from certain forms of endangerment. Later changes in the normative framework have also resulted in organizational changes in the way of critical infrastructure protection, as well as a special emphasis on other obligations related to the needs of the country's defense. It should be noted that this field is also considered in other countries in the region as an issue of importance for the country's defense.

However, in modern times, unlike developed European countries, the Republic of Serbia introduced the concept of critical infrastructure only in 2011 and in 2016 established an adequate legislative framework in accordance with the European standards. This is, among other things, important for achieving full membership in the EU. This can be seen through the provisions of national legislation, which have implemented positive European experiences in this field.

Key words: social self-protection, critical infrastructure, infrastructure sectors, national security, defense system

© 2021 The Authors. Published by *Vojno delo* (<http://www.vojnodelo.mod.gov.rs>).

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

