UDC: 327.5::351.88(4-672EU)
Review paper
Receved April 10, 2022
Accepted: April 28, 2022
Corresponding author: milijana.danevska@fpsp.edu.rs

EU INSTITUTIONAL CAPACITIES IN CRITICAL INFRASTRUCTURE PROTECTION

Milijana Danevska

Faculty of Business Studies and Law
"Union - Nikola Tesla" University, Belgrade, Republic of Serbia
e-mail: milijana.danevska@fpsp.edu.rs

Vladan Stanković

Faculty of Business Studies and Law
"Union - Nikola Tesla" University, Belgrade, Republic of Serbia
e-mail: vladan.stankovic@fpsp.edu.rs

Abstract: *Bearing in mind that the European Union is one of the key factors on the international scene when it comes to the protection of critical infrastructure (CI), it has launched a number of initiatives and research programs to protect CI. In this regard, the EU has studied various aspects of critical infrastructure protection, as well as the impact they have on damaging or destroying critical infrastructure on various segments of human activity, such as telecommunications, education, health, transport and others. The terrorist attacks in Madrid in 2004 and London in 2005 drew special public attention to the danger of attacks on critical infrastructures. Subsequently, the European Council asked the European Commission to prepare a comprehensive strategy and action plan to improve the protection of European Critical Infrastructure (ECI), which it did.*

Keywords: *European Union, EU institutions, critical infrastructure, protection, directives*

INTRODUCTION

The protection of critical infrastructure is extremely important for the well-being of the citizens of each country, because the survival and functioning of society and the

state as a whole often depends on the existence and functioning of individual (infrastructural) facilities and systems. Given that critical infrastructure is an important segment of both national security and European security, its protection is one of the priorities of every country. Therefore, states, especially in the past few decades, are taking special protection measures, which include, among other things, expanding the number of entities participating in that protection. Namely, due to its exceptional complexity and the range of facilities and systems on which the functioning of the state depends, it is difficult to define the concept of critical infrastructure. Also, defining the content and essence of the term CI differs from country to country, which is understandable given that each of them starts from its national interests and values. In the most general sense, CI "includes individual public and private sector institutions, distribution channels and 'networks' of persons and information that guarantee the smooth and continuous flow of people, goods, services, which is crucial for the stability of the country's economic and security system." Jakovljević: 2010) The category of 'critical infrastructure' includes telecommunications, electricity, gas and oil storage and transmission, banking and finance, transport, water supply, emergency services (including medical, police, fire and rescue services) and other institutions. "Jakovljević: 2010). Accordingly, CI includes all national capacities, services and information systems that are vital for the state and due to the inability to act or damage them could jeopardize national security, national economy, public health, public safety and efficiency of government. The issue of protection of CI is especially important because its endangerment can lead to a crisis, ie the emergence of crisis or emergency situations. Also, there is a possibility that crisis and emergency situations will lead to damage to CI. This indicates the interdependence of individual elements of KI, which can be seen in the example that if there is a threat to the operation of a particular hydropower plant, it may affect the work of certain health care institutions that are supplied with electricity from the plant.

The protection of the European Union's critical infrastructure is one of the important factors at the international level. The EU has launched many initiatives and programs to protect critical infrastructure. All member states participate in its protection, because if a critical infrastructure is disrupted or interrupted, it can easily be transferred to neighboring countries. A good example is complex infrastructures such as the energy network or gas pipeline, which are located throughout the EU and have vital nodes and critical assets in different Member States. Also, infrastructures belonging to the transport sector can be considered vital for two or more Member States, such as

transnational roads and tunnels set up at state borders and the like (Rehak, Markuci, Hromada and Barcova: 2016, p.7-12).

1. DEFINITION OF THE CONCEPT OF CRITICAL INFRASTRUCTURE

The problem in defining the term critical infrastructure is due to the wide scope that it can cover, as well as the great variety of content that is multidisciplinary in nature. The very term "infrastructure" can be defined as "the basic framework of a system or organization" while a multitude of definitions can be used for the phrase "critical infrastructure", because the term "critical" is variable and difficult to define. On the other hand, the complexity of the definition is influenced by the fact that the concept of critical infrastructure has changed over time, so it has sometimes remained unclear or insufficiently defined. Namely, the term protection of critical infrastructures (CIP) was first used by President Clinton in 1996, after the terrorist act on the Federal Building of Alfred P. Maraha in Oklahoma in 1995 (Executive Order, July 1996). This order highlights certain national infrastructures, which are of great importance for the United States, and whose disabling or destruction would have a great impact on defense, economic security and the well-being of citizens. NATO has a similar approach: "Defining critical infrastructure is a logical first step in protecting it, and therefore the definition used in a given country is often a reflection of that country's priorities. As there is no universally accepted definition, critical infrastructure is generally considered to be those facilities and services that are vital to the basic functioning of a society or without which society would be severely hampered "(NATO Commitment Reports: 2007). Regardless of the complexity of the definition, the notion of critical infrastructure is usually defined in one of two ways. The first method consists of listing all vital infrastructures, as was the case in the 2003 US Critical Infrastructure Protection Strategy, one of the first documents of its kind (The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, United States Government, Washington: 2003). From the scientific point of view, another approach is especially important, which defines criticality as a result of specific characteristics. In this case, certain (relational) properties of the system are determined, because the given system is critical in relation to other systems or entities. Namely, the system is critical for the second system when the first is necessary in order to continue the work of the second. Thus, the German National Strategy for Critical Infrastructure Protection defines

criticality as a relative measure of the consequences of disruption or failure of a function related to the delivery of goods and services to society (Bundesministerium des Innern Nationale Strategie zum Schutz Kritischer Infrastrukturen, Bundesministerium des Innern. Berlin: 2009, p.7). In this sense, critical infrastructure is the infrastructure needed to continue the operation of other major technical and / or social systems or needed to provide goods or services considered vital to the functioning of modern society (Lukitsch, Müller, Stahlhut: 2018, p.12).

There are several definitions of critical infrastructure, but all of them, in principle, refer to assets and property, which is crucial for the smooth functioning of the economy and society. Here are a few definitions. United States: "Critical infrastructure is a term that refers to the wide range of different assets and assets that are necessary for the daily functioning of social, economic, political and cultural systems in the United States of America (USA). Any disruption in critical infrastructure elements poses a serious threat to the proper functioning of these systems and can lead to property damage, human casualties and significant economic losses "(Murray: 2012). Australia: "Critical infrastructure is those physical facilities, supply chains, information technology and communications networks that, if destroyed or disabled for a long time, could significantly affect a nation's social or economic well-being, or affect Australia's ability to sustain national defense. and ensure national security "("Critical Infrastructure Emergency Risk, Management and Assurance "Emergency Management Australia, A Division of The Attorney Generals Department: 2003). European Union: "Critical infrastructure is the property, system or part thereof located in the territory of a Member State and which is necessary for the maintenance of key social functions, health, security, safety, economic or social well-being, and whose disruption or destruction would have a significant impact to a Member State ". European Union: "European Critical Infrastructure - ECI, means critical infrastructure located on the territory of a member state, whose disruption or destruction would have a significant impact on at least two member states. The significance of disturbances in the functioning of critical infrastructure elements should be assessed on the basis of interdependence criteria. This implies effects resulting from cross-sectoral dependence on other types of infrastructure "(Council Directive 2008/114 / EC). In general, the definition of critical infrastructure frameworks varies in many countries and depends on various specifics, ranging from political circumstances to geographical locations.

2. NORMATIVE REGULATION OF CRITICAL INFRASTRUCTURE IN THE EU

Following the terrorist attack in Madrid in March 2004, the Council of Europe in June 2004 asked the Commission to prepare a comprehensive strategy for the protection of critical infrastructure. In its response in October 2004, the Commission adopted a document relating to terrorism as a potential threat. The document, entitled "Communication from the Commission to the Council and the European Parliament on Critical Infrastructure Protection in the Fight against Terrorism: 2004", offers clear suggestions on what would improve European prevention., preparedness and response to a terrorist attack affecting critical infrastructure. The Council adopted the Commission's intention to propose a European Program for Critical Infrastructure Protection (EPCIP / EPCIP) and agreed on the Commission's arrangement for the Critical Infrastructure Warning Information Network (IMUKI / CIWIN). The European Critical Infrastructure Protection Program consists of three parts: the Identification and Designation Directive (ECI), the Financial Program and the Critical Infrastructure Warning Information Network (CIWIN). In November 2005, the Commission adopted a Green Paper on a European Program for Critical Infrastructure Protection (EPCIP) (Commission of the European Communities, Green Paper on a European Program for Critical Infrastructure Protection: 2005) which sets out its policy commitments to establish EPZKI and IMUKI. Also, this document provides a definition of critical information infrastructure protection, which states that "all programs and activities of owners, operators, manufacturers and users of infrastructure and regulatory bodies, which aim to ensure quality functioning, reduce damage and speed recovery of critical information infrastructures in case of failures or attacks on critical information infrastructure, together represent a program for the protection of critical information infrastructure "(Green Paper on a European Program for Critical Infrastructure Protection: 2005). The protection of critical information infrastructure should be viewed in the context of cross-sectoral connectivity, given that it permeates almost all other critical sectors and should be coordinated with the protection of all other critical infrastructure sectors (Marija Mićović: 2016, p.77).

An integral part of the EPZKI / EPCIP program is the 2008 Council of Europe Directive 2008/114 / EC. It defines critical infrastructure, common procedures for the identification and labeling of European critical infrastructure, a common approach to assessing the need to improve protection, as well as all risky approaches with the first

priority of the threat of terrorism. Directive 2008/114 / EC is the basis for the next steps in defining the criteria for critical infrastructure. Annex III of the same document lists the procedures that each Member State needs to implement, through several consecutive steps:

- **Step 1:** each Member State should apply sectoral criteria to create an initial selection of critical infrastructure within the sector;
- **Step 2:** each Member State should apply the definition of critical infrastructure, according to Article 2, point a) to potential European critical infrastructures identified after step 1. Significance is determined by using national critical infrastructure identification methods or by reference to cross-cutting criteria, at the appropriate national level. For infrastructures used to provide basic services, the availability of alternative infrastructure should be taken into account, as well as the duration of service interruptions / establishment;
- **Step 3:** Each Member State should apply the cross-border element for defining European Critical Infrastructure in accordance with Article 2, point b) to potential European Critical Infrastructures that have passed the first two steps of this procedure. The following step of the procedure applies to a potential European critical infrastructure that meets the definition. For infrastructures used to provide basic services, the availability of alternative infrastructure should be taken into account, as well as the duration of service interruptions / establishment;
- **Step 4:** Each Member State should apply cross-cutting, cross-sectoral criteria for the remaining European Critical Infrastructures. Cross-cutting, cross-sectoral criteria should take into account: the severity of the attack, and for the infrastructures used to provide basic services, the availability of alternative infrastructure, as well as the duration of service interruptions / establishment. If the potential European critical infrastructure does not meet the cross-cutting, cross-sectoral criteria, it will be considered that it is not a European critical infrastructure (Škero, Ateljević: 2015, pp. 192-207). In this way, the steps in determining the criteria for critical infrastructure are defined, the first step in identifying and determining the European critical infrastructure - ECI and the need to improve their protection is presented. It emphasized that it refers to the energy and transport sector, but also that it should be considered with special reference to the

assessment of the interaction of the sector, among other things, especially in relation to the information and communication technology sector. (Škero, Ateljević: 2015, pp. 192-207).

In March 2009, the Critical Information Infrastructure Protection Initiative (Communication for the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: 2009) established the European Public European Public Private Partnership for Resilience (EP3R) (EN3A: 2009) as a coordinating body for the European response to the cyber threat to the Union's critical information infrastructure. The role of the Working Groups established by this Partnership is to encourage the exchange of information and good practices, to enable the exchange of information and good practices in this area, and to identify basic preconditions for security and resilience in Europe. In the meantime, in 2013, the Critical Infrastructure Warning Information Network (CIWIN), a platform for exchanging information on common threats, weaknesses and appropriate measures and strategies to overcome risks to protect critical infrastructure, was created as a pilot project.. One of the 11 critical sectors considered by this platform is information and communication technologies (Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN)). Although primarily aimed at Member States, the CIWIN platform also provides access to authorities, organizations and experts from third countries in the framework of formal cooperation with the EU on activities related to the protection of critical infrastructure. (Rizmal, Radunović, Krivokapić: 2016, pp.25-26).

Also, in 2019, the 2008 Directive was revised, after which a new Critical Entity Resilience Directive (CER) was adopted in 2020, amending some old directives. The aim of European policy in this area is to ensure the functioning of the property, system or part of it, which can only be achieved on the basis of a common European framework for the protection of critical infrastructure.

Namely, the directive states that if the European Union wants to effectively protect Europeans, it should continue to reduce vulnerabilities, including the vulnerability of critical infrastructure, which is necessary for the functioning of its society and economy. Stating that the means of subsistence of European citizens and the good functioning of the internal market depend on various infrastructures, which are necessary for the maintenance of vital social and economic activities. To achieve this, the entities

providing the necessary services need to be resilient, ie able to resist, absorb, adapt and recover from incidents that could lead to serious, potentially cross-sectoral and cross-border disruptions (Directive of the European Parliament and of the Council on the resilience of critical entities: 2020).

This proposal aims to improve service delivery by increasing the resilience of critical entities, which are essential for maintaining vital social functions. This reflects recent calls for action by the Council and the European Parliament, which have encouraged the Commission to revise its current approach to better reflect the increased challenges for critical entities and ensure closer alignment with the Network and Information Systems Directive (MIS). Moreover, the proposal reflects national approaches in a growing number of Member States, which tend to emphasize cross-sectoral and cross-border interdependence. They also recognize the importance of resilience, in which protection is only one element along with risk prevention and mitigation, business continuity and recovery. Given that critical infrastructures are at risk of being potential targets of terrorists, the goal is to ensure the resilience of critical entities, which is also contributed by the goals of the recently adopted EU Counter-Terrorism Agenda.

Given the growing interconnectedness of infrastructures, networks and operators (managers) providing basic services across the internal market, and that the current critical infrastructure protection framework is not sufficient to meet all challenges, it is necessary to fundamentally change the approach to protecting specific means of strengthening the resilience of the critical entities that govern them. As evidenced by the 2019 evaluation of the ECI Directive, existing European and national measures face limitations in assisting operators (managers) trying to address operational challenges and vulnerabilities due to their interdependent nature. There are several reasons for this, first, operators (managers) are not fully aware or do not fully understand the implications of dynamic risks within their work. Second, resilience efforts differ significantly between Member States and sectors. Third, not all Member States recognize similar types of entities as critical (Directive of the European Parliament and of the Council on the resilience of critical entities: 2020).

In addition to jeopardizing the smooth functioning of the internal market, security risks and threats, especially those with cross-border and potentially pan-European action, can have serious negative consequences for citizens, businesses, governments and the environment. Indeed, at the individual level, security risks and threats can affect

Europeans' ability to travel, work and use public services such as healthcare freely. Finally, security threats, such as major power outages and serious accidents, can undermine security, fostering uncertainty and undermining trust in operators, as well as in the government responsible for their oversight and public safety.

This proposal reflects the priorities of the Commission for EU Strategy, which calls for a revised approach to critical infrastructure resilience that better reflects the current situation and anticipates future risks, as well as increasing interdependence between different sectors and the relationship between physical and digital infrastructure.

The proposed directive replaces the ECI Directive (2008), takes into account and builds on other existing and envisaged instruments. The proposed directive represents a significant change compared to the ECI Directive, which applies only to the energy and transport sectors and which focuses exclusively on safeguards and provides a procedure for identifying and designating ECIs through cross-border dialogue.

First of all, the proposed directive would have a much broader sectoral scope, covering ten sectors, namely energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration and space. Second, the directive provides a procedure for Member States to identify critical entities using common criteria based on national risk assessments. Third, the proposal sets out the obligations of the Member States and the critical entities they identify (Directive of the European Parliament and of the Council on the resilience of critical entities: 2020).

CONCLUSION

Bearing in mind that critical infrastructure is a complex system, we believe that a holistic approach should be taken in its protection. Given the challenges, risks and threats that countries face, it is necessary that all countries within the European Union are in agreement on the definition and protection of CI. This is regulated by the EU Directive on Critical Infrastructure Protection from 2008, which is a good model and provides an opportunity to take over certain solutions, especially in the field of regulating public-private partnerships. The Critical Infrastructure Resilience Directive of 2020 complemented the importance of CI protection by emphasizing critical infrastructure resilience. Also, the said Directive expands the critical infrastructure

sectors, provides for a procedure for the identification of critical entities using common criteria and sets out the obligations of the Member States and the critical entities they identify.

Critical infrastructure protection is a concept that is still under development. Namely, there is no standard model of protection at the global or European level. The directives of the European Commission are framework and significant changes can be expected in the near future. The state of development at the level of the European Union is such that the Union is also looking for its identity in this area. Significant efforts and resources are being invested to arrange it conceptually and practically. One of the possible solutions is to regulate this area through international and European standards that would prescribe the best practice in the field of critical infrastructure protection (Keković, Ninković: 2020, p. 104).

REFERENCES

1. Bundesministerium des Innern Nationale Strategie zum Schutz Kritischer Infrastrukturen, Bundesministerium des Innern. Berlin, 2009
2. Commission of the European Communities, Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17.11.2005.), COM (2005) 576 final, p. 19, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576
3. Communication for the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, (2009), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52009DC0149
4. Council Directive 2008/114/EC of 8 Decembar 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 L, pp. 345-375, 23.12.2008.
5. Critical Infrastructure Emergency Risk, Management and Assurance, Emergency Management Australia, A Division of The Attorney Generals Department, 2003.
6. Critical Infrastructure Warning Information Network–CIWIN https://ec.europa.eu/home-affairs/networks/critical-infrastructure-warning-information-network-ciwin_en

7. Directive of the European Parliament and of the Council on the resilience of critical entities, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN
8. Lukitsch K., Müller M., Stahlhut C. Criticality in: Engels I., J. (ed.): Key Concepts for Critical Infrastructure Research, Springer, Wiesbaden, Germany, 2018
9. NATO Commitettee Reports, 2007, https://www.nato-pa.int/document/2007-162-cds-07-e-rev1-critical-infrastructures-jopling-report
10. Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN) (2008), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52008PC0676
11. Rehak D., Markuci J., Hromada M., Barcova K. (2016), Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system, International Journal of Critical Infrastructure Protection, 14, https://reader.elsevier.com/reader/sd/pii/S1874548216300774?token=BE378878EF6A284FD514F332A868BA59568015A047F77C637F260C91E200BB535C56965A598A15D6F23A601B6E5BBE54&originRegion=eu-west-1&originCreation=20211223153417
12. T.G.A.T. Murray, (2012), Critical Infrastructure protection; The vulnerability conudrun, Telematics and Informatics, vol. 29, no. 1
13. The Communication from the Commission to the Council and the European Parliament on "Critical Infrastructure Protection in the fight against terrorism, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52004DC0702
14. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, United States Government, Washington, 2003
15. Јаковљевић, В. (2010), Ресурси критичне инфраструктуре и њихов значај за управљање ванредним ситуацијама, Годишњак Факултета безбедности, Београд
16. Кековић, З., Нинковић В., (2020) Заштита критичне инфраструктуре - системски приступ, Центар за анализу ризика и управљање кризама, Београд
17. Мићовић М. (2016), Безбедносни аспекти функционисања критичне инфраструктуре у ванредним ситуација, докторска дисертација, Београд
18. Ризмал, И., Радуновић, В., Кривокапић, Ђ. (2016), Води кроз информациону безбедност у Републици Србији, Центар за евроантланске студије, Београд
19. Шкеро, М., Атељевић, В. (2015), "Заштита критичне инфраструктуре и основни елементи усклађивања са Директивом Савета Европе 2008/114/ЕС", Војно дело, 3/2015