HARMONIZATION OF LEGISLATIVE EFFORTS FOR PROTECTION OF CRITICAL INFRASTRUCTURE WITHIN THE EUROPEAN UNION AND POTENTIAL EFFECTS FOR CANDIDATE COUNTRIES

Marjan GJUROVSKI[1]
Vesna POPOSKA[2]
Gjorgi ALCHESKI[3]

Abstract

Critical infrastructure and critical entities, as providers of basic services, play an indispensable role in maintaining vital social functions or economic activities in the internal market in the union's increasingly interdependent economy. It is therefore essential to establish a Framework of the Union in order to simultaneously strengthen the resilience of critical entities in the internal market by establishing harmonized minimum rules and assistance with the help of coherent and dedicated support and surveillance measures. Those processes already started occurring , facing growing and continuous threats of today's world. Directive (EU) 2022/2557 - formally adopted by the co-legislators on 14 December 2022, introducing a number of additional critical infrastructure protection (CIP) measures and replacing Council Directive 2008/114/EC - also known as ECI Directive, is supposed to be transposed into national legislations of EU member states in the upcoming two years. In parallel, update of NIS directives came in power as many different sector related legal documents. For the candidate countries, it is additional effort of essential meaning, especially for North Macedonia that is a NATO member. This paper aims to provide an orientation framework toward the key achievements that are supposed to be met for effective protection of critical infrastructure at national level.
Keywords: critical infrastructure, entities, harmonization, legislation.

INTRODUCTION

European critical entities are more interconnected and interdependent, which makes them stronger and more efficient but also more vulnerable in case of an incident. Russia's war of aggression against Ukraine has brought new risks, physical and cyber-attacks, often combined as a hybrid threat. The sabotage of the Nord Stream gas pipelines and other recent incidents made it clear that the resilience of the EU critical infrastructure is under threat (EC 2022).

[1] Faculty of Philosophy, Institute of security, defense and peace studies, University SS. Cyril and Methodius- Skopje, Republic of North Macedonia, marjan.gjurovski@fzf.ukim.edu.mk.
[2] Faculty of Law, International Vision Universit- Gostivar, Republic of North Macedonia, vesna.poposka@vizyon.edu.mk.
[3] Faculty of Philosophy, Institute of security, defense and peace studies, University SS. Cyril and Methodius - Skopje, Republic of North Macedonia, gjorgji.alcheski@tav.aero.

The separation of critical infrastructure as a security and operational term is a relatively new phenomenon that became especially relevant after the Russian attack on Ukraine, covering mostly energy and transport systems, but also water systems and traffic infrastructure. However, even though the term is new, it does not mean that critical infrastructure is a new phenomenon. On the contrary, every social order in every age of humanity had its own critical infrastructure, that is, systems essential for social functioning - water supply, production and food supply, certain road corridors, etc.

The development of technology imposed the trend of improvement of living conditions by creating modern systems and services which they provide. The effects of their action for a short period they exceeded the capacities of the national borders. Today, these systems and services are interconnected, intertwined and largely dependent on each other, that is, it is evident their interdependence (Bakrevski, Mislohevska and Alcheski 2017).

In the changed security environment, critical infrastructure is a legitimate object of protection that must be recognized by the system as such through the imperative of the norm, that is, the legal framework. It is a security determination that generates the creation of new legal norms and the interpretation of existing ones in a different light and requires the application of legal analogy. Most of the critical infrastructure today is privately owned, that brings new challenges to national security systems. Consequently, regardless of where a particular segment of infrastructure is located - the state itself may no longer be able to provide the critical infrastructure in its entirety and may be heavily dependent on the private sector for this purpose. Corporations that own a significant part of the critical infrastructure are constantly expanding the market and the activity, striving to achieve dominance and profit. Much of the property is in risky areas.

Thus, while the term "critical infrastructure" is relatively new in the international community, this does not mean that its existence has not been regulated or treated in an international context so far. For example, international humanitarian law contains a number of provisions for the protection of civilian facilities or facilities that can have dual purposes (hospitals, dams, water supply systems) and although it does not point to them as critical infrastructure, they de facto represent it, which is why they enjoy special protection. From sources of international law, it is difficult to separate special norms that treat critical infrastructure as such. In the context of national law, the situation is much easier if an individual state directly regulates critical infrastructure protection. In this context, it is also important to which legal tradition belongs the state concerned: continental or Anglo-Saxon, due to the sources of law to which each of them is invoked. In a changed security environment, critical infrastructure is an object of legitimate protection that must be recognized by the system as such through the imperative of the norm, i.e. the legal framework. Events of the near past have a direct impact on the creation of certain legislative norms, which are constantly being upgraded.

DEFINING CRITICAL INFRASTRUCTURE

For the first time, defining critical infrastructure is made by the United States. In May 1998, President Bill Clinton issued a Presidential Directive PDD-63 on critical infrastructure protection. This act states that certain parts of national infrastructure are crucial to the national and economic security of the United States and to the well-being of its citizenship and that it is necessary to take steps for protection.

Gradually, as the global context developed, a growing number of countries approached the practice of regulating the protection of critical infrastructure as a separate category. The definition of critical infrastructure is different for any state or international organization, but in general, critical infrastructure is defined as such on the basis of the same or similar characteristics.

Furthermore, to understand the concept of critical infrastructure, it is very important to take into account sectoral interdependence and close interaction. Vital sectors are interconnected and interactive, leading to the creation of new vulnerabilities and critical points. Such interdependence can manifest as physical, cyber, geographical and logical (Rinaldi 2004).

The European Union defines critical infrastructure through 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, as well as Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (EU 2022).

The newly adopted Directive od 2022, goes a step further and defines not just the critical infrastructure, but the critical entities- entirely new term that is supposed to take into consideration and accent the systematic interdependencies. Critical entities are entities providing essential services that are crucial for the maintenance of vital societal functions, economic activities, public health and safety, and the environment. They need to be able to prevent, protect against, respond to, cope with and recover from hybrid attacks, natural disasters, terrorist threats and public health emergencies (Council of the EU 2022).

In the Tallinn Manual, critical infrastructure implies physical or virtual means and means that are in the jurisdiction of the state and are so vital that their disabling or destroying them can weaken national security, the economy, public health and security or the environment (CCDCOE 2017).

Different states define critical infrastructure in different manner and sectors may vary from country to country. For example, in Germany it is defined as: "Critical infrastructure implies the organizational structure and objects vital to society, so that their degradation or deficit will result in shortcomings, cause a significant reduction in supply, public order violations or other consequences" (Federal Republic of Germany 2009).

In United Kingdom it is "Critical national infrastructure covers those means, services and systems that support the economic, political and social life of the United Kingdom, the importance of which is such that loss can cause major loss of lives;

have a serious impact on the national economy; have other serious social consequences for the community; or be of immediate care to the national government" (NPSA 2023).

Netherland recognizes two categories of critical infrastructure, of which category A includes: transport networks and national transmission systems for gas and electricity, nuclear materials and a water supply system, which are treated with a higher level of protection, and in Category B with a lower level of protection include regional distribution of gas and electricity, air traffic and maritime traffic, larger reserves of the petrochemical industry, police, government services dependent on relevant and available date bases and information systems, communication systems among emergency services and the financial sector (The Hague Security Delta 2015).

PROTECTION OF CRITICAL INFRASTRUCTURE

Each critical infrastructure has unique characteristics, operating models and risk profiles, which have institutional significance and specialized expertise in relation to the specified sector. The enabling environment is one of the key factors for the extent of resilience of each critical entity. Some of them are: the interdependence, aging, relaying to the cyber domain, expenses and the quality and sharing of intelligence information.

The most important pillar of the EU program is the adoption of Council Directive 2008/114/EC ie 2022/2557 which calls on member states to identify and designate European critical infrastructure and assess the need to improve their protection. All Member States have implemented the Directives by establishing a process to identify and designate European critical infrastructures in the energy and transport sectors.

The European Union in Directive 2008/114 (EC 2008) , under "protecting critical infrastructure", implies "all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise threat, risk or vulnerability. Given the nature and characteristics of critical infrastructure as such, protection is reduced to all hazards approach.

Regardless of the specifics that there are different opinions on the effective improvement of security, the Directive is a striking example as an example of a legal instrument and a policy for the protection of national critical data. This was leveled with concrete actions, as created at the national level for policy management.

A new Directive 2022/2557 was adopted at the end of 2022 and it introduced the term "critical entities". Member states are given two years to comply with it.

The Lisbon Treaty largely introduced the solidarity clause with Article 222, which calls on member states to act together and help each other in the event of a terrorist attack or a natural or man-made disaster. In addition, Lisbon treaty introduced the additional competence formula for the EU in Article 196 to encourage cooperation between member states in order to improve the efficiency of protection and rescue systems against natural or man-made disasters (European Union 2011).

In addition, the competence for the internal market from Article 114 of the TFEU enables the adoption of sectoral measures for security and protection.

As part of the EU's cybersecurity strategy adopted in 2013, the Directive on achieving a common high level of network and information security, known as the NIS Directive, was adopted in 2016. The deadline for national transposition by EU member states was 9 May 2018. The directive has three parts that refer to:

- Building national capacities, in each member country individually;
- Cross-border cooperation: cross-border cooperation between EU countries.
- National supervision of critical sectors: EU member states should supervise the cyber security of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health and financial sector), ex-post supervision for critical suppliers of digital services (internet exchange points, domain name systems, etc.).

On 16 January 2023, the Directive (EU) 2022/2555 (known as NIS2) entered into force replacing Directive (EU) 2016/1148. ENISA considers that NIS2 improves the existing cyber security status across EU in different ways by:

- creating the necessary cyber crisis management structure (CyCLONe)
- increasing the level of harmonization regarding security requirements and reporting obligations
- encouraging Members States to introduce new areas of interest such as supply chain, vulnerability management, core internet and cyber hygiene their national cybersecurity strategies
- bringing novel ideas such as the peer reviews for enhancing collaboration and knowledge sharing amongst the Member States
- covering a larger share of the economy and society by including more sectors which means that more entities are obliged to take measures in order to increase their level of cybersecurity (ENISA 2023).

APPLICABLE LEGAL FRAMEWORK

To extract the applicable legal framework for the protection of critical infrastructure, an analysis of the context is necessary.

In the context of "all hazards approach", it is necessary to note that critical infrastructure and its protection are often considered in a strategic, security and operational context, but not in a normative context, although it is the legal framework that is the basis for the operationalization of protection in each field.

From the sources of international law, it is difficult to single out specific norms that treat critical infrastructure as such. In the context of national law, the situation is much easier if the individual state directly regulates the issue of interest. In that context, it is also important to which legal tradition the country in question belongs: continental or Anglo-Saxon, because of the sources of law that each of them refers to.

Considering the fact that a large part of the critical infrastructure has been privatized, the provisions of the civil law will apply to the operators, especially in the area of ownership and legal obligations. Most often, if it is about foreign direct investments, they have a special regime of protection and some aspects are regulated by both international investment law and national law. International investment law will

undoubtedly find its role. Given the increasing impact of global warming and natural disasters, international environmental law is yet to be the center of gravity of the debate.

The regulatory bodies and agencies and the by-laws enacted by them have a special role in the national legislation. Criminal legislation, on the other hand, has a special protective and preventive role that was elaborated separately. All actors must find their place in the crisis management system, based on centralized management and decentralized execution. The obligation of standardization, safety protocols and occupational safety must also be respected accordingly in every sphere.

That's why, it is necessary to standardize the normative framework, i.e. for the national legal system to recognize and recognize critical infrastructure as a value through the adoption of the first law for the protection of critical infrastructure.

THE CASE OF NORTH MACEDONIA

North Macedonia is NATO member country since 2020, as well as EU candidate country. Although the two cornerstone directives are supposed to be met by member states only, it is of crucial importance to be considered as part of the *acquis*- the law of the EU that should be transposed into national legal systems of the candidate countries.

To put the critical infrastructure at the centre of the enlargement process, it is necessary to discuss the timetable for implementation of the proposals in the Directive on Resilience of Critical Infrastructure and the Cybersecurity Directive, both of which were published as final drafts in 2022, designed for member states. The CER requires national strategies, risk assessment, identification of critical infrastructure and reporting of incidents. Critical Entities Resilience Groups will be set up to enable regular cross-border cooperation on infrastructure in 10 sectors, including transport and energy. Complementing the wide scope of the CER, NIS 2 covers cyber-defense aspects in more detail. NIS 2 also places more obligations on EU member states regarding supervision and enforcement requirements and establishes a Cyber Crises Liaison Organization Network (EU-CyCLONe). In the context of the sabotage of Nord Stream 1 and Nord Stream 2, there is an urgency about implementing these directives. Although the CER and NIS 2 directives are meant for the EU member states, they should be open to candidate states obtaining observer status in the Critical Entities Resilience Groups and EU-CyCLONe. (SCEEUS 2023).

The Republic of North Macedonia has not yet defined its critical infrastructure in law, with a by-law or national strategy, but according to the program for the approximation of the law of the European Union 2015 – 2017.

However, it is an issue to be overcome very soon. Since 2022, Ministry of Defense introduced the Committee MkNATO 2023, dedicated on policy making for the essential reforms in the sector. Within this committee, there is a Subcommittee for the preparation of a law for the protection of critical infrastructure that drafted the Law on critical infrastructure with the support of international consultantsand does attempt to balance the basic principles of the 2008 Directive and the 2022 Directive.

The draft law is in the final phase of preparation within the Ministry of defense and should enter into force before the end of the year (MOD 2023).

THE NEED FOR HOLISTIC APPROACH

Considering the fact that a large part of the critical infrastructure has been privatized, the provisions of the civil law will apply to the operators, especially in the area of ownership and legal obligations. Most often, if it is about foreign direct investments, they have a special regime of protection and some aspects are regulated by both international investment law and national law. International investment law will undoubtedly find its role. Given the increasing impact of global warming and natural disasters, international environmental law is yet to be the center of gravity of the debate.

The regulatory bodies and agencies and the by-laws enacted by them have a special role in the national legislation. Criminal law, on the other hand, has a special protective and preventive role that was elaborated separately.

All actors must find their place in the crisis management system, based on centralized management and decentralized execution.

The obligation of standardization, safety protocols and occupational safety must also be respected accordingly in every sphere.

States' practice that has proven successful is to integrate the protection of critical infrastructure into broader national security strategies as a separate segment, applying an "all hazards" approach emphasizing the threat of terrorism, and establishing mechanisms for prevention, early warning, risk management and effective crisis management. Therefore, the legal framework that addresses all these issues must be properly harmonized.

International law is implemented in national legislation through appropriate mechanisms, which are ultimately translated into appropriate normative solutions. If the first element of legal certainty is the good legal solutions, the second element is the consistency in their implementation and the sustainability of the fiscal implications they produce.

This implies that the legal regime for the protection of critical infrastructure from modern security threats will be the smallest common content of a set of legal instruments. International and national law will meet here, guided by the risk assessment for the relevant environment - from terrorism to natural disasters and climate change.

At the same time, it must not be forgotten that the law exists to absorb the social context and that it must be flexible enough to be able to adapt to the dynamic development, and to allow progress from "the law as it is, to the law as it should be (*de lege lata - de lege ferenda*)", while fully preserving the democratic benefits of liberal societies, regardless of the challenges they face.

CONCLUSIONS

In a national context for the Republic of Northern Macedonia, the adoption of a Law on (Protection of) Critical Infrastructure is extremely important, but this will not solve the problem and provide effective protection unless a functioning system for civil protection and early prevention is provided. At least two laws need intervention and amendments - the Law on Crisis Management and the Law on Protection and Rescue. In this constellation, it is difficult to call the crisis management system a system. Shortcomings prevail more than solutions, and therefore it is necessary, when we talk about its reforms, to keep in mind that the reform here will have to represent a completely new installation based on experience and best practices adapted to the local and regional context. In addition to harmonising the national legal framework, harmonisation with international standards and implementation of the obligations and recommendations arising from the membership of the Republic of North Macedonia in international groups and associations is necessary. It is also necessary to refine the rights and obligations of private security companies to provide and place them in the critical infrastructure protection system. It is extremely important to build, on the basis of law, coherent and effective public policies. The partial approach solves one, two or a few problems, but opens up a whole pleiade of others. Only then will a society that is resilient and whose vital functions are provided without violation of liberal values and human rights and freedoms will be built (Poposka 2022).

Threats will continue to grow and mutate. Effective protection lies in prevention and strengthening of society - and in strengthening the legal framework in that segment. It implies legal amendments and the application of best practices, with the establishment of the entire institutional framework resulting from it, as well as the effect of the fiscal implications. And the best legal solution cannot be effective without an implementation mechanism and without predicting appropriate fiscal implications for it.

Ensuring fully critical infrastructure is an impossible mission, but that does not mean that improving its security should not be a continuous process. The most important thing in this process is to build resilience or resilience, both critical infrastructure and society in its entirety. NATO was the leader of the idea of resilience (elasticity/resilience) as a step forward in effective protection.

BIBLIOGRAPHY

Bakrevski, O., Mislohevska. T., Alcheski, Gj. 2017. *Protection of critical infrastructure*. Chamber of private security of North Macedonia. Available at https://obezbeduvanje.org.mk/wp-content/uploads/2020/12/Zashtita-na-kriticna-infrastruktura-za-web.pdf.

CCDCOE. 2017. Tallinn Manual on the International Law Applicable to Cyber Warfare.

Council of the EU. 2022. EU resilience: Council adopts a directive to strengthen the resilience of critical entities. Available at https://www.consilium.europa.eu/en/press/press-

releases/2022/12/08/eu-resilience-council-adopts-a-directive-to-strengthen-the-resilience-of-critical-entities/.
ENISA. 2023. Supporting the implementation of Union policy and law regarding cybersecurity. Available at https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.
EU (20022) Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114.
European Comission. 2022. Critical Infrastructure: Commission accelerates work to build up European resilience. Available at Critical Infrastructure: Commission accelerates work to build up European resilience.
European Council. 2008. 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. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114
European Union. 2002. Treaty of the European Communirt available a https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12002E/TXTandfrom=EN
Europen Union. 2011. The Treaty of Lisboa. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12007L%2FTXT.
Federal Republic of Germany. 2009. National strategy for protection of critical infrastructure. Available in English at http://ccpic.mai.gov.ro/docs/Germania_cip_stategy.pdf.
MOD. 2022. Petrovska about the Draft Law on Critical Infrastructure: Our approach to the construction of an efficient system for the protection of critical infrastructure is thorough and without improvisations. Available at https://mod.gov.mk/petrovska-about-the-draft-law-on-critical-infrastructure-our-approach-to-the-construction-of-an-efficient-system-for-the-protection-of-critical-infrastructure-is-thorough-and-without-improvisations/.
NPSA. 2023. Critical national infrastructure, available at https://www.npsa.gov.uk/critical-national-infrastructure-0.
NPSA. 2023. Centre for protection of the national infrastructure of the UK available at https://www.cpni.gov.uk/critical-national-infrastructure-0.
Poposka, V. (2022. *International legal aspects for protection of critical infrastructure against contemporary security therates.* International Vision University Series Publishing.
Rinaldi, S. M. 2004. "Modeling and simulating critical infrastructures and their interdependencies". In: *Proceedings of the 37th Hawaii International Conference on System Sciences*. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.1206andrep=rep1andtype=pdf.
SCEEUS. 2023. EU Eastern Enlargement: Preparing for Current and Future Threats Through Inclusive Crisis Management and Resilient Critical Infrastructure. Available at

https://sceeus.se/en/publications/eu-eastern-enlargement-preparing-for-current-and-future-threats-through-inclusive-crisis-management-and-resilient-critical-infrastructure/.

The Hague Security Delta. 2015. Securing critical infrastructure in the Netherlands: Towards a national testbed. Available at https://www.thehaguesecuritydelta.com/media/com_hsd/report/53/document/Securing-Critical-Infrastructures-in-the-Netherlands.pdf.