IX INTERNATIONAL SCIENTIFIC PROFESSIONAL CONFERENCE
SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTICE (SeCMan)
- IX INTERNATIONAL FORUM „SAFETY FOR THE FUTURE 2023" -
29th and 30th September 2023, Belgrade, Republic of Serbia

CRITICAL INFRASTRUCTURE PROTECTION IN SOME BALKAN COUNTRIES IN COMPARISON WITH BOSNIA AND HERZEGOVINA

Zeljko Zoric[1]
[1]Sector Security, Street Sinise Mijatovica 9, Banja Luka, Republic of Srpska, Bosnia and Herzegovina, zoriczeljko1@hotmail.com

Received: 10th July 2023
Accepted: 10th August 2023

Professional paper

Abstract: *Frequent social changes, acts of terrorism and war, climate changes, often lead to temporary or permanent damage to critical infrastructure. Precisely because of the consequences, critical infrastructure protection is a frequent topic of discussion in the scientific and professional public. The first step in action when it comes to critical infrastructure protection is the adoption of legal acts what will define critical infrastructure as well as the measures for its protection. In this regard, the countries surrounding Bosnia and Herzegovina have already come a long way, driven by the real internal needs and EU requirements. Entities in Bosnia and Herzegovina, as well as the existing District, have not taken significant steps in the field of critical infrastructure protection. In this paper, the legal solutions for critical infrastructure protection in Bosnia and Herzegovina, Croatia and Serbia are presented using the method of comparison and content analysis.*

Key words: *critical infrastructure, law, protection, comparison*

1. INTRODUCTION

With the establishment of the first social communities, certain values arose that had to be protected, the values whose damage or destruction would question the survival of the entire community, With the civilization development, certain measures also developed, that is, ways of protecting social values, which today we call by a unique name – critical infrastructure.

The beginning of the 21st century marked, among other things, a renewed focus on critical infrastructure protection, especially in the West, as a result of increased concern for the provision of basic needs such as enery and transport. However, instead of the earlier focus on the danger of large-scale armed conflicts, "new" uncertainties are increasingly coming to lights, primarily because of the increasing critical infrastructure complexity and interdependence. Therefore, instead of the danger of conventional military conflict, increasingly present cyber threats in the conditions of interconnected and networked infrastructures are being considered. (Milosavljevic & Komazec, 2021).

Critical infrastructure networking and its distribution certainly crosses national borders, and therefore its protection have a different significance. Namely, contemporary threats very often

surpass national borders and therefore affect the multinational response. An obvious example is climate change, which has led to significant change in the form of increasingly frequent heavy rainfall and long-lasting droughts in an unexpectedly short period of time. These changes threaten infrastructure to a great extent in almost all countries and therefore require a unique response. Even though we try very hard to pay attention to these causes, it is also necessary to return to somewhat neglected threat to infrastructure, and those are the ones caused by war operations. The current military conflicts between Russia and Ukraine have brought to surface the threats to all infrastructure segments. According to the available data, which derive from the official reports of the parties involved in this conflict, it is evident that infrastructure destruction is brutal and neither side takes into account the consequences that remain, on civilians and nature. Electric power system facilities, roads food production, etc. are particularly at risk. The new situation represents a serious test for the adopted protocols for critical infrastructure protection from threatening phenomena, regardless of the time, place and manner of their manifestation. Large countries can allow themselves to independently develop a critical infrastructure protection system, even though it may turn out not to be a good solution.

The recent earthquake in Turkey has shown that this territorially large and populous country is not able to respond independently to such an accident that caused significant damage to the infrastructure in all aspects. The European Union, with its infrastructure, certainly represents a serious challenge to protect it from various endangerment forms. The existing system certainly has its advantages and disadvantages when it comes to measure implementation in real situations of endangerment. The recent corona virus epidemic, as well as the current situation in Ukraine, as two diametrically opposite causes, put the existing EU protection measures to a serious test.

Protection measures against the corona virus have shown that they are not very effective, i.e., that EU member states made decisions very quickly that were not in accordance with the EU's unique measures. Almost overnight, the member states re-established a hard border in places where it had been abolished some time ago. The wartime destruction of infrastructure in Ukraine is certainly a serious concern for the EU and will influence the revision of the existing critical infrastructure protection system. Countries that are now members of the EU, but have an intention of becoming one, such as Serbia, adopt laws and measures that follow the recommended standards and develop critical infrastructure protection system that would be isomorphic with the system that exists in the EU. When it comes to Bosnia and Herzegovina with its entities and districts, it is evident that it represents an "isolated island" in Europe without any organized measures to protect critical infrastructure.

2. CRITICAL INFRASTRUCTURE PROTECTION IN THE EUROPEAN UNION

The European Union has recognized the importance of critical infrastructure protection, i.e., the consequences that would occur if it were threatened. The latest threat to critical infrastructure, as a consequence of the corona virus pandemic, put the existing critical infrastructure protection system to a serious test. It has been shown that critical infrastructure is no longer and cannot be the responsibility of one state only, i.e., we are talking about critical infrastructure whose protection is regionally connected. In order for the EU to adopt uniform measures and procedures, it was necessary to adopt a uniform definition of critical infrastructure, which reads: "Critical infrastructure is an asset, system or a part of it, located in the territory of a member country and which is necessary for the maintenance of key social functions, healthcare, safety, security economic or social well-being, and the disruption or destruction of which would have a significant impact on the member country".

European Program for Critical Infrastructure Protection (EPCIP) from December 12, 2006 set a general framework for activities aimed at improving critical infrastructure protection in all EU countries and in all relevant sectors of economic activity.

Four main focus areas of EPCIP were then developed:

1. Procedure for European critical infrastructure identification and designation and assessment of the need to improve their protection is detailed in Council Directive 2008/114/EC;

2. Measures designed to enable the EPCIP implementation, including action plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP (Critical Infrastructure Protection) expert groups at the EU level, the CIP information exchange process and identification and interdependency analysis;

3. Financing CIP-related measures and projects that focus on prevention, preparedness and management of terrorism consequences and other security-related risks for the period 2007-2013;

4. EPCIP external dimension development (Kekic, 2019).

Directive 2008/114/EC is the basis for the next steps in defining criteria for critical infrastructure. Annex III of this Directive lists the procedures, which each member country should implement, through several consequent steps. EU critical infrastructure protection is also based on critical infrastructure protection in the fight against terrorism (COM (2004) 702 final, October 20, 2004); Green Paper on the European Program for Critical Infrastructure Protection (COM (2005) 576 final, November 17, 2005); Communication from the Commission on the European program for critical infrastructure protection (COM (2006) 786 final, December 12, 2006). Working document of the Commission service on a new approach to the European program for critical infrastructure protection – Additional insurance of European critical structures (SWD (2013) 318 final, 28/08/2013).

Strategic agenda for 2019-2024 which was adopted by the European Council in June, requires a comprehensive approach to protect Europe from malicious cyber activities and hybrid threats. The European Commission assessed the 2008 Directive on critical infrastructure protection. The assessment shows the evolution of threats facing Europe. The evaluation also emphasizes that the EU's approach towards critical infrastructure protection must be flexible and risk-based to reflect the threats and vulnerabilities critical infrastructure is likely to face in upcoming decades. The assessment suggests that there are additional sectors that member states consider worthy of additional protective actions at the European level. Based on the evaluation findings, there are reasons to examine the scope of the EU critical infrastructure framework with the aim of including additional sectors (Kekic, 2019). If the corona virus pandemic tested the critical infrastructure protection system in the EU, the conflict in Ukraine certainly influenced the need to raise a serious question about the critical infrastructure protection functionality in the EU. That there have been serious changes in the understanding, definition and protection of critical infrastructure is clear from the "introduction" of the NATO structure and forces in critical infrastructure protection. NATO and the EU launched a work group to strengthen critical infrastructure in response to the "attack" on the Nord Stream gas pipelines and Russia's use of energy as a weapon in early 2023. This work group consists of NATO and EU experts tasked with identifying key threats to critical infrastructure, to assess vulnerabilities and an appropriate response. This is, at the same time, critical infrastructure protection militarization in which there is no place for civilian planning and management, which again questions numerous previously adopted documents at the EU level that do not take into consideration critical infrastructure only. That such a work group is a concept

previously prepared, for something new in the future, can be concluded from the fact that it has not yet been proven who is guilty of sabotage on the Nord Stream.

3. CRITICAL INFRASTRUCTURE PROTECTION IN CROATIA

With the Law on Critical Infrastructure Protection from 2013 and 2022, Croatia took over the EU regulations contained in Council Directive 2008/114/|EC from 2008 on European critical infrastructure identification and determination and the assessment of the need to improve their protection. Croatia adopted the Law on Critical Infrastructures (Croatian Parliament, 2013), the Decision on determining the sector from which central state administration bodies identify national critical infrastructures and lists of critical infrastructure sector sequence (Government of the Republic of Croatia, 2013), Rulebook on Methodology for creating critical infrastructure risk analysis operations (DUZS director, 2013). In order to improve and align with international standards, in 2016, a new Rulebook based on the ISO 31000:2009 standard (instructions and guidelines for risk management) was adopted and applied.

Laws and by-laws regulate the critical infrastructure risk management area, with regards to: the exposure of the Republic of Croatia to dangers, both of natural origin and those caused by technical and/or technological processes, which include exposure to terrorist activities, both in real and in cyberspace, that Croatia is particularly sensitive to threats to its critical infrastructures because its resources do not allow it to fully develop alternative/redundant systems, and this sensitivity is increased by the connection and interdependence of numerous sectors both at the national level and with critical infrastructure sectors both at the national level and with critical infrastructure sectors of neighboring and other countries, that this area represents the backbone of national and public security and sustainable development and progress of key interest, both for the population/individuals, as well as for the overall economy, social activities and the country as a whole. In July 2018, the Croatian Parliament adopted the Law on Operator Cybersecurity of Key Services and Digital Service Providers, which transposed Directive 2016/1148 of the European Parliament and the Council of the EU on measures a high common level of network and information system security throughout the Union into Croatian legislation, which regulates the area of critical infrastructure information and communication security. Achieving the highest level of critical infrastructure and population safety and protection is determined by the first strategic goal of the National Security Strategy of the Republic of Croatia (Government of the Republic of Croatia, 2017). The State Administration for Protection and Rescue of the Republic of Croatia has adopted the Rulebook on the methodology for the critical infrastructure risk analysis operations, which "establish the guidelines, criteria and benchmarks for the critical infrastructure operation identification and risk analysis, as well as the holders and their obligations of critical infrastructure business risk analysis which is an integral part of the risk assessment process." The Rulebook was published in the Official Gazette, 47/2016.

4. CRITICAL INFRASTRUCTURE PROTECTION IN SERBIA

The Law on Critical Infrastructure Protection regulates national and European critical infrastructure identification and determination of the Republic of Serbia, competence and responsibility of authorities and organizations in the field of critical infrastructure and information, reporting, providing decision support, data protection, management and supervision in the field of critical infrastructure. In order for the Law to be fully applicable, the Regulation on the criteria for the critical infrastructure identification and manner of reporting it was adopted in the Republic of Serbia in 2022. The criteria according to which critical infrastructure is identified are determined based on the assessment of the consequences that may occur due to critical infrastructure disruption or destruction, as well as based on the consequences that may occur in the event of threats to critical infrastructure. The criteria

established by this regulation are the basis for determining critical infrastructure in the Republic of Serbia.

One of the main reasons for the adoption of the Law on Critical Infrastructure ("The Official Gazette of the Republic of Serbia", 87/2018) is the absence of a single law in this area and the need to unify it. The term 'critical infrastructure' is mentioned in several different documents, first of all, in the Law on Emergency Situations, then in regulations and strategies, but also in the Law on Information Security and the Law on Private Security. The law first defines the terms included in the content, starting with what the critical infrastructure sector is, then the way in which identification, determination, protection is carried out, who the operators are, what the security plan, is liaison officer and finally what European critical infrastructure is. The principles of action contained in this Law apply to competent authorities, organizations and citizens, and these subjects are obliged to comply with them. The principles are exhaustively enumerated in the Law, namely the principles of integrated approach, responsibility and protection against various types of threats, the principles of continuous planning for critical infrastructure protection, data and information exchange and data protection (Micovic, 2020).

Of course, the newly adopted law has been harmonized with the EU directives concerning critical infrastructure, while retaining a certain independence in defining critical infrastructure and the way of responding to its threat. Some of the laws concerning critical infrastructure are: the Law on Railways ("The Official Gazette of the Republic of Serbia", no. 41/2018); the Law on Safety in Railway Traffic ("The Official Gazette of the Republic of Serbia", no. 41/2018); the Law on Interoperability of the Railway System ("The Official Gazette of the Republic of Serbia", no. 41/2018); the Law on Electronic Communications ("The Official Gazette of the Republic of Serbia", no. 44/2010, 60/2013 – Constitutional Court Decision, 62/2014 and 95/2018 and other laws); the Law on Water ("The Official Gazette of the Republic of Serbia", no. 30/10, 93/2012 and 101/2016); the Law on Meteorological and Hydrological Activities ("The Official Gazette of the Republic of Serbia", no. 88/2010); Strategy for Electronic Communications Development ("The Official Gazette of the Republic of Serbia", no. 68/10); the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business ("The Official Gazette of the Republic of Serbia", no. 94/2017); the Law on Electronic Commerce ("The Official Gazette of the Republic of Serbia", no. 41/2009 and 95/2013); the Law on Confirmation of the Convention on High-tech Crime ("The Official Gazette of the Republic of Serbia", no. 19/2009); the Law on Private Security ("The Official Gazette of the Republic of Serbia", no. 104/13); the Law on Organization and Competence of State Bodies for the Fight against High-tech Crime ("The Official Gazette of the Republic of Serbia", no. 61/2005 and 104/2009); the Law on Information Security ("The Official Gazette of the Republic of Serbia", no. 6/2016 and 94/2014); the Law on Data Confidentiality ("The Official Gazette of the Republic of Serbia", no. 104/2009). The methodology and contents of the disaster risk assessment and the protection and rescue plan were published in "The Official Gazette of the Republic of Serbia", no. 87/2018.

Critical infrastructure existence and protection is nothing new to the Republic of Serbia, as it has been dealing with this issue successfully for many years, especially in the part where critical infrastructure can be threatened by natural disasters and various accidents. By introducing the new law, Serbia only "unified" numerous provisions related to critical infrastructure, which were defined in some other laws.

5. CRITICAL INFRASTRUCTURE PROTECTION IN BOSNIA AND HERZEGOVINA

When it comes to critical protection infrastructure in Bosnia and Herzegovina, with its entities and Brcko District, has not yet done anything, nor are there any indications that much will happen in the near future. Bearing in mind that Bosnia and Herzegovina shares similar critical infrastructures with its neighboring countries, as well as the causes of threats to critical infrastructures, it is clear that quality legal solutions and their application in practice can be reached in a short time. The reason for the absence of quality response as far as Bosnia and Herzegovina is concerned, can be found in political misunderstanding or lack of desire to protect critical insurance approaches in the optimal and recommended way. One of the reasons, but not the main one, is the way Bosnia and Herzegovina is organized and functions. Brcko District has no adopted documents related to critical infrastructure protection, and neither does the Federation of Bosnia and Herzegovina. In the Republic of Srpska, the situation is somewhat more favorable. There is an adopted law, but nothing further has been done in accordance with that law. The Law on Critical Infrastructure Safety in the Republic of Srpska, was adopted in 2019 (The Official Gazette of the Republic of Srpska, no. 58/19). That there was no further implementation of the Law is evident from the following:

- According to the provisions of this Law, Government of the Republic of Srpska was obliged to pass a bylaw regulation on the procedure for checking the critical infrastructure subjects and facilities with six months from the date of this Law entering into force – it was not done;

- According to the provisions of the law, the heads of the Republic's administrative body were obliged to adopt certain sectoral measures within eighteen months form the date of this Law entering into force – it was not done;

- According to the provisions of the law, Ministry was obliged to adopt the sectoral measures to adopt Methodology which would refer to critical infrastructure[a] within nine months from the date of this Law entering into force;

- According to the provisions of the law, the republic's administrative bodies were obliged to propose critical infrastructure from their jurisdiction's sector and their level of criticality, within six months from the Methodology adoption date – it was not done.

If the Law were to be implemented now, the effect would certainly be very weak. This is due to the fact that the five-year cycle since the adoption of the law is coming to an end, i.e., the period when everything done so far should be reviewed. The audit would give a special review of the effectiveness of the measure applied to critical infrastructure facilities, thus creating preconditions for a possible change in the existing legal solutions, The lost time and failure to understand the need to protect critical infrastructure in Bosnia and Herzegovina only shows that the society as a whole is not ready to accept and respond to the need to protect critical infrastructure, and thus, in addition to its own community, it also puts neighboring countries in a disadvantageous situation. Due to this attitude towards the critical infrastructure protection, neighboring countries will have to engage additional resources in order to prevent

[a] The methodology was done by Ministry of the Interior of the Republic of Srpska and in cooperation with the Civil Protection Republic Administration, but it was graded with a certain degree of secrecy. The essential question relates to the reasons for "secrecy" for the methodology used. The methodology that refers to critical infrastructure protection or is directly related to critical infrastructure facilities in neighboring countries is a publicly published document in The Official Gazette and publicly available to everyone. Author's comment.

the threatened infrastructure in Bosnia and Herzegovina from “spilling over” onto their countries as well.

7. CONCLUSION

The adoption of measures and their redefinition regarding the identification and critical infrastructure facility protection measures clearly indicate social awareness development of the need for mutual action, very often at the regional level, in order to be able to speak with certainty about its protection readiness in all circumstances. Croatia, as a member of the EU, adopted the Law that fully implements the EU Directive 2008/114/EC, while respecting the specificities at the national level. Servia, even though it is not a member of the EU, accepts the mentioned Directive, and it can be said that it regulates the legal solutions related to critical infrastructure in a better way. This is a consequence of constant change monitoring in a country and environment that may affect critical infrastructure, as well as many years of experience in this field. Bosnia and Herzegovina, by not adopting any documents, at the level of the Council of Ministers, districts or entities, only complete a general picture that indicates that Bosnia and Herzegovina is a creation that is not able to take care of elementary things that should be it its/their jurisdiction. This inert attitude puts the neighboring countries in a disadvantageous position. Namely, in addition to managing the state of their critical infrastructures, they are “forced” to think about the same in Bosnia and Herzegovina. This is due to the fact that it is expected that the critical infrastructure threat in any part of Bosnia and Herzegovina, due to an inadequate response, may spread to the neighboring countries’ territory

REFERENCES

Kekic, C. (2019). Direktiva Saveta o utvrdjivanju i oznacavanju evropske kriticne infrastrukture i proceni potrebe unapredjenja njene zastite. Evropsko zakonodavstvo, Institut za medjunarodnu politiku i privredu, Beograd, 22-37.

Milosavljevic B. Komazec N. (2021). Kriticna infrastruktura i drustvena odgovornost, Istrazivacki centar Banja Luka, Zbornik radova, „Zastota kriticne infrastrukture-obaveze drzava i mogucnosti privatnog sektora bezbjednosti“, Naucno-strucna konferencija sa medjunarodnim ucescem, Banja Luka

Micovic, M. D. (2020). Specificnosti kriticne infrastrukture u Republici Srbiji. (Elektronski izvor).

Istrazivacki centar Banja Luka. (2021). Zbornik radova, „Zastita kriticne infrastrukture-obaveze drzava i mogucnosti privatnog sektora bezbjednosti“, Naucno-strucna konferencija sa medjunarodnim ucescem, Banja Luka

Narodne novine Republike Hrvatske broj 47/2016

Sluzbeni glasnik Republike Srbije broj 87/18 i 69/22

Sluzbeni glasnik Republike Srpske broj 44/2010, 60/2013, 62/014, 95/2018, 87/201841/2018, 58/19.

https://federalna.ba/nato-i-eu-pokrecu-radnu-grupu-za-zastitu-kriticne-infrastrukture-isulo NATO i EU pokrecu radnu grupu za zastitu kriticne infrastrukture, 11.01.2023.