ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOCTORAL (PhD) THESIS

MILICA SIKIMIĆ

Contemporary Security Framework for Critical Infrastructure Protection – the Case Study Implementation in Bosnia and Herzegovina

Supervisor: Dr. habil. János Besenyő

DOCTORAL SCHOOL ON SAFETY AND SECURITY SCIENCES

27 October 2024

Public Defence Committee:

President:
Prof. Em. Dr. Livia Cveticanin

Secretary:
Dr. Richard Pető

Members:
Dr. habil. Rudolf Nagy
Dr. habil. Ágota Drégelyi-Kiss
Dr. habil. András Tóth

Reviewers:
Dr. habil. Tibor Farkas
Prof. Dr. Saša Mijalković

Date of the Public Defence:
2025

Contents

INTRODUCTION

1. Problem and subject of research

Different approaches to definition and classification indicate that critical infrastructure most often includes, but is not limited to, food, water, agriculture, health and emergency services, energy, transport, information and telecommunications, banking and finance, chemical plants, defense industry, post and distribution of goods. Threatening any of the mentioned sectors can cause energy and economic instability, dysfunctionality of information systems and serious disruption in the free movement of people, transportation of goods and provision of services. Due to the interconnectedness and interdependence of vital infrastructure systems, a disruption in the operation of one of the systems can produce the so-called cascading impact in other sectors. Thus, the consequences of disruptions in the provision of services to critical entities can be of local, regional, national, or even supranational scale, where neighboring countries are most at risk. Therefore, since the beginning of the 21st century, the European Union has been working on harmonising policy in the field of security of vital infrastructures, with the aim of comprehensive protection of the European community.

In the southeast of the European continent lies the Western Balkans, a geopolitical entity comprising several countries that are not members of the European Union. The countries of the Western Balkans have close and unbreakable economic, production, energy, security and other relations with the European Union. The Republic of Serbia, Bosnia and Herzegovina, Montenegro, Republic of North Macedonia and Albania are countries that directly border at least one European Union member state. Furthermore, all the mentioned countries have clearly expressed their intentions to join the European community.

After the Stabilisation and Association Agreement entred into force and the European Commission responsed positively to Bosnia and Herzegovina's application for accession to the European Union, a series of activities has been initiated to fulfill obligations and address challenges on the European path. One of those challenges is the establishment of a modern and efficient state framework for the security of critical infrastructure. Bosnia and Herzegovina does not have a unified strategy or law regulating the area of critical infrastructure at the state level, but the initiated activities at the normative level indicate an alignment with European guidelines in the field of critical infrastructure security and the resilience of critical entities. As for the action and institutional measures, critical infrastructure in Bosnia and Herzegovina has not been officially identified or designated yet. Consequently, the infrastructure of importance

for the European community has neither been established nor protected within the borders of this country.

The security of critical infrastructure is a priority task for the security and defense system of every state and supranational communities. Therefore, the central problem addressed in this thesis will be: *How to establish an effective security framework in Bosnia and Herzegovina that will enable reaching the necessary level of security and resilience of the infrastructures whose functioning is of vital national and european importance?*

The formulated problem needs to be approached by seeking answers to these questions:

- What are the determinations of the security policy of Bosnia and Herzegovina?
- What are the normative and legal foundations for the security of critical infrastructure in Bosnia and Herzegovina?
- What are the institutional capacities for the security of critical infrastructure in Bosnia and Herzegovina?

The subject of this research refers to the analysis of all factors that determine the construction of a modern framework for the security of critical infrastructure in Bosnia and Herzegovina. We will explore the current situation in the area of critical infrastructure security in Bosnia and Herzegovina, the determination of public policy actors in the area of security, the operation of the national security system and the fulfillment of existing international/European standards during the implementation of national legislation that regulates the management of critical infrastructure. *The more specific research subject is aimed at investigating the normative framework, institutional and organisational capacities in the security system of Bosnia and Herzegovina, from the aspect of security of critical infrastructure*.

2. Research objectives

The scientific objective of the research is:

- scientific description and classification of critical infrastructure as a determinant of the national and European security;
- scientific analysis of the security system and security policy of Bosnia and Herzegovina, from the aspect of critical infrastructure security.

The practical objective of this research is to, based on theoretical knowledge and empirical results:

- provide a more comprehensive and objective overwiev of the existing normative and institutional characteristics of modern security systems with a special emphasis on the protection of critical infrastructure in a country,
- propose public policies in the field of security and practical solutions for establishing a modern security model for the protection of critical infrastructure, and
- propose directions for improving the legal and institutional framework for the security of critical infrastructure in Bosnia and Herzegovina, taking into account both European standards and the real needs and possibilities.

3. Hypotheses

In accordance with the stated objectives, the following research hypotheses have been formulated.

First hypothesis: The protection of critical infrastructure is organised and implemented primarily at the national level.

Second hypothesis: The capacities and mechanisms of the security system determine the efficiency and functionality of critical infrastructure.

Third hypothesis: The protection of critical infrastructure in Bosnia and Herzegovina is not sufficiently effective and needs to be improved by adopting new normative and institutional solutions.

Fourth hypothesis: The security framework for strengthening the resilience of critical infrastructure in Bosnia and Herzegovina is being developed according to the guidelines of the European Union.

4. Justification and determinants of research

The scientific and social justification of the research arises from the objectives to be achieved, which are reflected in expanding and deepening knowledge on all issues related to

improving national and European security in the field of critical infrastructure. The expected results and scientific contribution stem from the security, political, economic and social importance of the topic, which is becoming increasingly relevant and important, but scientifically unexplored.

The timing of the research was concluded on January 1, 2024, and any subsequent changes and statistical data are not included in the dissertation.

Disciplinary determination of the research subject: The research subject is primarily located in the field of security studies. However, this research encompasses other areas of other social and humanistic studies and scientific disciplines such as legal, political, military, criminal investigations and criminology, as well as technical and information sciences, giving this investigation a multidisciplinary character.

5. Research methods

The formulated problem and research subject, along with the set objectives and assumed hypothetical framework, indicate the need for a multi-method approach and complementary analysis of available and newly created data sources. Therefore, the following methods will be used in the study:

- content analysis, including historical and dogmatic-legal methods,
- comparative method, and
- research method.

The *content analysis* method will be used to study domestic and foreign literature with the aim of scientific description of critical infrastructure, security policy and framework for its protection. *The historical method* will be employed to gain the necessary background of the researched problem, that is, to discover how and when the concept of critical infrastructure was created. The historical approach explains the evolution of policies and mechanisms for the protection of critical infrastructure. *The dogmatic-legal method,* i.e. the method of interpreting legal norms, is necessary for the interpretation of positive legal regulations governing the area of critical infrastructure security.

The comparative method will enable a comparative analysis of the existing state in the normative, organisational and functional aspects of critical infrastructure security in the

national security systems of specific countries, i.e., Bosnia and Herzegovina, developed countries and neighboring countries.

The test method will be used for the purpose of the implementation of empirical research, employing semi-structured interviews (in-depth interviews). The data will be collected from responsible persons, executives, employees of one of the facilities of vital importance. Other public and private sector individuals directly involved in the establishment, organisation and implementation of critical infrastructure protection will also be interviewed. Primarily, those will be employees of the government and private sector. The questionnaire is listed in Annex 1.

In the study, data will be analysed from various sources, and experience records will be systematically created from existing data sources, such as:

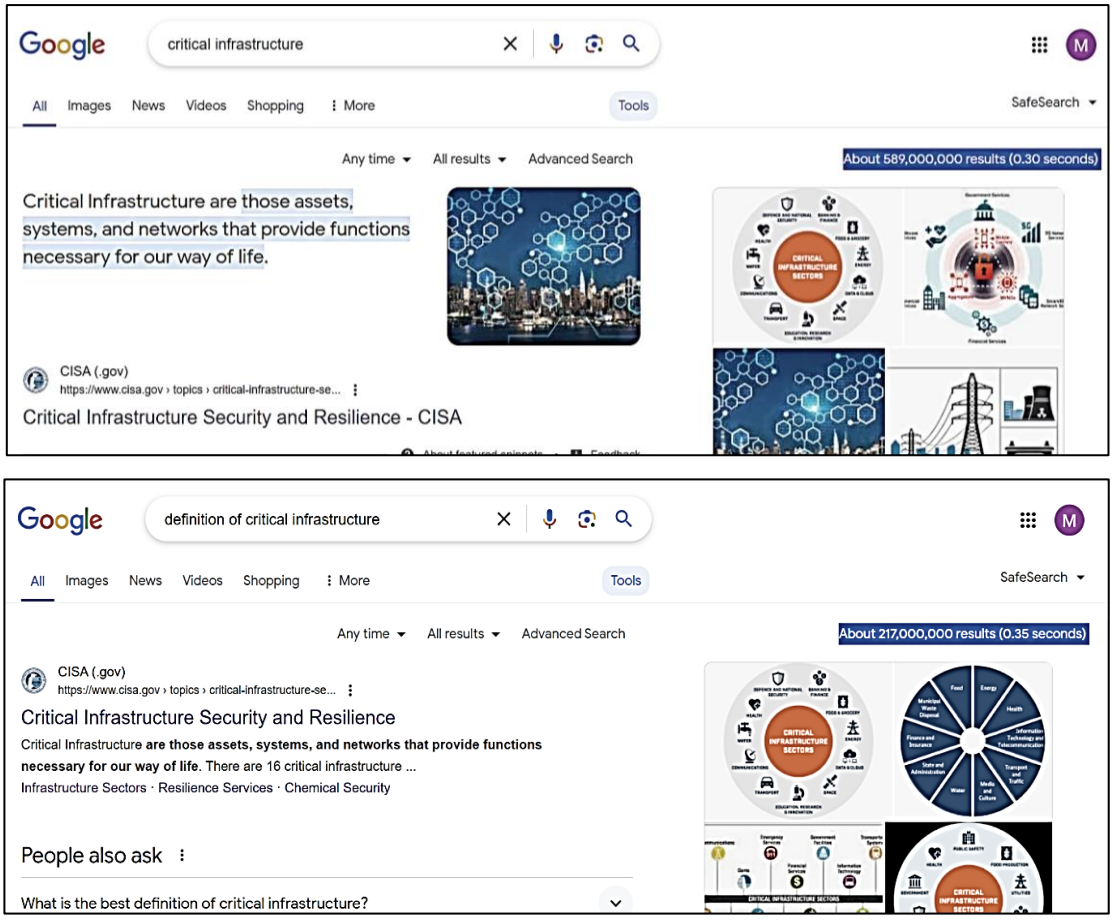
- scientific and professional papers by domestic and foreign authors directly dealing with security policy in the field of critical infrastructure,
- scientific and professional research projects in the country and abroad,
- positive legal regulations at the national, regional and international level,
- institutional sources such as statistical reports from local, state, regional, non-governmental and other relevant institutions, and
- international documents such as conventions, protocols, international agreements, directives, action plans and other acts.

Through these methods, we intend to arrive at facts that will form the basis for drawing conclusions, confirming or rejecting the proposed hypothetical framework.

CRITICAL INFRASTRUCTURE AS A DETERMINANT OF NATIONAL AND EUROPEAN SECURITY

1. Conceptual determination of critical infrastructure in safety and security studies

The terms "infrastructure" and "critical infrastructure" in scientific-professional communication, everyday use and political vocabulary are extremely frequent and their frequent use causes different associations (De Felice, Baffo & Petrillo, 2022). A Google search for the phrase "critical infrastructure" gives 589 million results in less than 1 second, while a search for the phrase "definition of critical infrastructure" gives 217 million results. What kind of infrastructure is it and why is it so important and difficult to ensure its adequate protection?



Picture 1: Results of a Google search for the phrase "critical infrastructure" and "definition of critical infrastructure"[1]

[1] Search results on 2024, May 11.

The meaning of the term “infrastructure” is not entirely determined and is subject to different interpretations by researchers who primarily see it through the prism of their disciplinary and home field of research (De Felice, Baffo & Petrillo, 2022). As a result, there are numerous definitions and determinations of certain concepts that are conditioned by the approach and needs of the author. The technical sciences are dominated by the engineering approach which differs in its characteristics from the approach in the natural sciences, and both significantly differ from the approach in the social sciences, i.e. in the corpus of security studies. Nevertheless, the word “infrastructure” originated from the Latin compound *infra - below, beneath* and *structure - assembly, composition, arrangement*, signifying a term used in the broadest sense in the social sciences to describe auxiliary parts of a broader system without which the system would not function (Komarčević, 2018; Amidzić & Sikimić, 2024).

The term “critical infrastructure” is relatively recent (from the end of the 20th century), but the importance of the functioning of vital systems was also known to the ancient Romans and Greeks. The Roman Empire developed systems of road infrastructure, aqueducts (water and waste water system) and food supply. It was these systems, especially the famous Roman aqueducts, that enabled the foundation and preservation of such a large and powerful empire. Aqueducts served the needs of citizens’ water supply and were originally constructed underground. However, when the first above-ground aqueducts were built, they became the target of enemy attacks (Newbill, 2019). The destruction of the water supply system seriously threatened the functioning, strength and power of the empire, and the vulnerability and protection of this vital infrastructure became a matter of national security and defense.

The strength and power of the ancient Greeks was undermined by the seizure of the source of food supply (grain) by the enemy, leading Athens to sent over thirty thousand soldiers to prevent the seizure of grain (Brown, 2006; Hale, 2009). The identification and targeting of vulnerable infrastructure also had a major impact in World War II when the bombing and destruction of the German railway system caused the country’s economy to collapse, facilitating the continuation of the war for the Allied forces (Newbill, 2019).

Although the destruction of important infrastructures in security and defense studies is primarily studied in the context of the impact on military operations and the maintenance of state power, negative effects on the civilian population must be acknowledged as an indispensable aspect of the analysis (e.g. the lack of drinking water and food, insufficiency or lack of health care results in the suffering of the population). The first official determination of the infrastructure that must be provided is related to the Report of the President’s Commission

in the United States of America in 1997. Infrastructure is "The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole" (The Report of the President's Commission, 1997: Appendix B-2). Furthermore, critical infrastructures are "Infrastructures which are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security" (The Report of the President's Commission, 1997: Appendix B-1). The document emphasises the need to raise awareness about the crucial importance of protecting critical information infrastructure and, in that context, the insignificantly low role of military power (The Report of the President's Commission, 1997).

Determinations of critical infrastructure in Europe have been in existence since 2004 (Lazari, 2014: 2-3). In 2008, *the 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* was adopted (hereinafter Directive 2008/114/EC) (Council Directive 2008/114/EC, 2008). Through this document, the geographical factor of critical infrastructure is introduced, and according to Directive 2008/114/EC "critical infrastructure means an asset, system or a part thereof located in Member States which is essential the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" (Council Directive 2008/114/EC, 2008: Article 2 (a)). In December 2022, this Directive was repealed, and the initiated activities will be directed toward the *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* (hereinafter Directive 2022/2557). For the purposes of the dissertation, we will use the definitions of *infrastructure, essential services and critical entities* from Directive 2022/2557.

"*Infrastructure* means an asset, system or part therof, which is necessary for the delivery of an essential service" (Directive 2022/2557, Article 2(4)). We notice that the emphasis in the identification of vital infrastructure is on the element of criticality, and not on the definition. Criticality criteria cover all infrastructure in all sectors and are mostly bilaterally oriented. On the one hand, these criteria emphasise the purpose of the infrastructure by defining essential services that the infrastructure delivers. "*Essential service* means a service which is

essential for the maintenance of vital societal functions or economic activities" (Directive 2022/2557, Article 2(5)). On the other hand, criticality criteria emphasise the severity or the effects of the disruption or destruction of a given infrastructure on society. This means that infrastructure is critical because its loss would significantly hinder the functioning of the state and society (Lazari, 2014: 3). Therefore, it is necessary to determine critical entities, i.e. public or private entities that provide one or more essential services which depend on the infrastructure in the territory of a country (Directive 2022/2557, 2022).

The currently valid guidelines of the European Union do not recognise the term "critical infrastructure", but rather infrastructures and critical entities. Nevertheless, it is to be expected that *critical infrastructure* will be a part of scientific, professional, political, educational and university vocabulary for some time to come. Although there is no universally accepted definition, critical infrastructure is generally understood as those facilities and services that are vital to the basic operations of a given society, or those without which the functioning of a given society would be greatly impaired (De Felice, Baffo, & Petrillo, 2022). In the field of safety and security studies, critical infrastructure is the infrastructure whose destruction or endangerment can cause a serious disruption in the free movement of people, transportation of goods and provision of services, negatively affect national and regional security, health and lives of people, property, environment, economic stability and continuous functioning of institutions.

2. Classification and sectors of critical infrastructure

The values that will be protected are related to the needs and interests of each community, and the areas from which critical infrastructure is determined are quite broadly defined. Since the beginning of the last century, national lists of critical infrastructure sectors have followed the evolution of the complexity of infrastructure, human and social needs whose analysis helps to understand the differences between countries. Also, important events that significantly disrupted the regular cycle of critical infrastructure (such as 9/11) had a major impact on the change of the list of critical infrastructure sectors. The national security priorities of a country are often expressed through the classification of critical infrastructure and the designation of certain critical sectors.[2]

[2] In the dissertation, we take the sectoral approach for the reason that most European countries have adopted this approach. In addition to the sectoral approach, a systemic approach or a classification of critical infrastructure which is based on its functions can be found. Additionally, there is a classification of critical infrastructure based on elements that are building components of the sector, such as elements at the local level, elements at the regional

In the United States, "the Nation's critical infrastructure provides the essential services that underpin American society" and currently 16 sectors are designated "whose assets, systems, and networks (physical or virtual) are considered so vital to the United States that their incapacitation or destruction would had a debilitating effect on security, national economic stability, public health or safety or any combination thereof." According to data from the official website of the *Department of National Security*, critical infrastructures in the United States of America today are classified into the following sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, water and wastewater systems and transportation systems (Critical Infrastructure Sectors, 2023). This list is regularly updated.

Regarding the classification of critical infrastructure in the European Union, it was initiated in Directive 2008/114/EC. Two sectors with sub-sectors were identified, namely the energy sector and the transport sector. Within the energy sector, the sub-sectors included electricity, oil and gas, while in the transport sector, the sub-sectors comprised road transport, rail transport, air transport, inland waterways transport, ocean and short-sea shipping and ports (Council Directive 2008/114/EC). Currently, the official classification of entities providing essential services is presented in the Annex of the Directive 2022/2557. The energy sector encompasses the sub-sectors such as electricity, central heating and cooling, oil, gas and hydrogen, while the transport sector includes air, water, rail and road transport. In addition to the two mentioned, the Annex defined seven more sectors, namely: banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration and space (Annex to the Directive 2022/2557, 2022).

By summarising the content analysis of scientific and professional literature, we find that critical infrastructure most often includes, but is not limited to, the following: food and water supply, health and emergency services, energy (electrical, nuclear, gas and oil, dams), transport (air, road, rail, ports, waterways), information and telecommunications, banking and finance, utilities, chemical plants, defense industry, environmental protection, manufacturing, storage and transportation of hazardous materials, post and distribution of goods, space and research, education, national monuments and other cultural values. The following is an

level, elements at the state level and elements at the international level (see more in Simić, Jurišić, Maksimović, & Jovičić, 2020: 12-17).

explanation of certain entities, objects and networks that are most often represented in the classifications of critical infrastructure.

Safe food means a sufficient amount of healthy food (Mijalković & Bajagić, 2023). Critical infrastructure for water supply ensures a constant flow of drinking water, industrial water, water for agriculture, for electricity generation, the availability of water for firefighting and other needs. This sector includes water sources, reservoirs and storage facilities, water mains and other delivery systems, water filtration, cleaning and treatment systems (waste water handling), pipelines, cooling systems and other delivery mechanisms that provide water. Plants and facilities for the production, processing and storage of food are also critical infrastructure, and, according to available data in the United States, this sector accounts for one fifth of the country's total economic activity (Critical Infrastructure Sectors, 2023). Health, emergency medical interventions, police work to protect life and property, civil protection and fire services can be included in the critical infrastructure sector of emergency services. This system is based on the interconnectedness of institutes, hospitals, health centers, institutions, private medical practices, laboratories, pharmaceutical companies and pharmacies, the supply chain for these institutions, etc. Its external connection is essential with all other emergency services such as police, army, fire service and civil protection (Simić, Jurišić, Maksimović, & Jovičić, 2020: 101).

The energy sector is singled out as particularly critical because it operates to support other sectors and almost all industries rely on this sector. This sector comprises electricity companies which perform the function of supply, distribution networks, entities in the electricity market providing storage or consumption management services, oil pipelines, oil production facilities, gas production and distribution facilities, etc. (see more: Annex to the Directive 2022/2557, 2022). The necessity of transporting raw materials and products emphasises the interdependence of the energy sector with the transport sector. The transport system consists of several types of traffic: land (road, rail, pipeline), water (sea, river, lake, canal), air, postal and telecommunication traffic. Within a country, the transport infrastructure represents an extremely complex system with a pronounced degree of connectivity at different levels (vertically and horizontally), and a failure in one element can manifest itself through a negative impact on other elements. Furthermore, traffic as an economic activity enables greater mobility of the population and is an important segment in the functioning of modern society (Achillopoulou, Mitoulis, Argyroudis, & Wang, 2020).

A system is as strong as its weakest link and, in terms of the functioning of critical infrastructure, that link is usually information and communication technologies. Information critical infrastructure encompasses infocommunication systems, which are inherently critical infrastructure elements, and at the same time are necessary for the operation of other critical infrastructure elements (telecommunications, computers and software, internet, satellites, etc.). These infrastructures are interconnected to form global critical networks, thereby linking the vulnerabilities of individual components of the system. The work of emergency services, military command, educational system, financial system, etc. depends on the functionality of information and communication critical infrastructure. Therefore, the protection of information critical infrastructure is an interdepartmental and even intergovernmental task (Information Technology Sector, 2023).

Financial and banking services represent a vital component of critical infrastructure because they manage trillions of dollars, ranging from individuals' payroll deposits to the transfer of huge amounts to support large global enterprises, organisations and governments. Examples of components of these entities include retail and commercial organisations, investment institutions, brokerage firms, trading firms and reserve systems, government operations and support activities (America's cyber defense agency, 2023).

The accumulation of waste generated by the daily needs and activities of people can have negative consequences on public health and other ecosystems. Therefore, it is necessary to properly remove different types of waste, and this activity can be classified as a critical infrastructure for communal activities. Nevertheless, the production, storage, use and transport of potentially dangerous chemicals are mostly within the scope of critical chemical infrastructure sector, and some countries even designate a special sector for critical nuclear infrastructure (Critical Infrastructure Sectors, 2023).

Due to its significant importance for the state, the defense system requires constant planning, development, maintenance and improvement of capacities and mechanisms. The critical infrastructure of the defense system is distributed across a large number of locations where military complexes are located, and the elements of the critical infrastructure of this sector include machanisation, equipment, technical means, communication systems and more (Komarčević, 2018: 280-289).

Upbringing and education implies an acceptable and affordable education for citizens of an international entity, but it also involves openness to the acquisition of knowledge by

individuals, interest communities, groups and organisations in other countries. The protection of this system includes a wide range of protection of national interests and the need for educational workforce. It is essential that in crisis situations this system has reference capabilities for "distance learning" and IT support for implementing this method of education (Simić, Jurišić, Maksimović, & Jovičić, 2020).

In the critical infrastructure sector for national monuments and other cultural values, assets are essentially physical structures and include the operational staff and visitors who may be impacted by a terrorist attack or all-hazard incident. The need for its protection also was determined during the rise of political, religious and other tensions when the destruction of historical monuments, archival materials, cultural monuments and religious objects can cause unrest among citizens, provoke protests of one or another interest group and destabilise the security of environment. However, in Christianity, the church is therefore the guardian of the national culture and identity. In Montenegro, from December 28, 2019 until the middle of March 2020, peaceful protest gatherings known as "litije" were held every day with the aim of expressing citizens displeasure regarding new regulations affecting the property of the Orthodox Church. These protests directly affected parliamentary elections and political change in the state (see more in Arandjelović, 2022; Šljivić, 2021).

In addition to the mentioned classification, each country can, in accordance with its needs, perform a different classification and determine other areas where critical infrastructure will be designated.

3. Critical infrastructure as a determinant of national security

The national state exists in conditions of multiple interweaving of political, economic, social, religious and other interests and relations of numerous sovereign and non-sovereign actors. Nevertheless, national security remains a central concept in security sciences, and the state is the fundamental provider of security (Mijalković, Nacionalna bezbednost, 2018).

The essence of international relations lies in the inequality of states as their subjects, and the amount of state power determines whether that state will achieve various types of its goals (Mijalkovski & Đorđević, 2010). The strength of the influence of international relations and foreign policy on national security can also be seen through the obligation of the state to organise the national security system in accordance with the signed bilateral and multilateral international agreements. Finally, the national power of a certain state is the ability to make changes through the coordinated rational use of its resources within and beyond its borders

which represent a state of optimal protection of national vital values and ensure their sustainable development (Mijalkovski & Đorđević, 2010: 25).

The functioning of critical infrastructure is a necessary condition for maintaining the regular state of national security (Alexandru, Vevera, & Ciuperca, 2019), that is, for the functioning of society, the state and its participation in international relations. Facilities, systems and networks of vital importance must operate in all conditions, both in peacetime and wartime, as well as in emergency situations. When critical infrastructure is threatened, negative impacts spread to internal and external security, the health and lives of people, property and the environment, and ultimately, national security is threatened.

Regardless of the type of political system, the leadership of each state identifies key national goals and the future state it aims to achieve. Each state proclaims national values of vital importance and guarantees them with its legal order, defining the possibility of using mechanisms of state coercion. In principle, the concept of national security is linked to four groups of values which are crucial for the existence of the state as an international subject and the existence and development of society. These are: survival, territorial integrity, political independence and the quality of life. Operationalisation of these strategic values identifies values such as a healthy environment, energy stability, economic and social prosperity, information resources, rights and security of citizens and social groups (Mijalković, 2018). By comparing, we observe that national values are contained in key services, i.e. critical infrastructure sectors Amidzić & Sikimić, 2024).

Considering that countries have different geographical, political, socio-economic and other factors, it is clear that the definition, as well as critical infrastructure sectors, cannot be identical in all countries and regions (Trbojević, 2018). Therefore, critical infrastructure is primarily determined at the national level. States, as subjects of international relations, possess the largest number of human, material, technical and organisational capacities for the protection of critical infrastructure (Sikimić, 2022c). The absence of national institutional mechanisms and legal regulations can have destructive effects on the security of the entire planet, but the functioning of critical infrastructure primarily impacts the security of a country (Alexandru, Vevera, & Ciuperca, 2019). In addition to the societal and state security, national security also includes the participation of the state in international and global security. Internal legal norms regulating a state's security must be aligned with the general norms of international

law, which, in the context of critical infrastructure, presents regulatory alignment (Sikimić, 2022c) and key aspects of protection beyond national borders.

The efficient functioning of all segments of society, the state, government bodies, legal and natural persons, and the enhancement and preservation of national power represent the fundamental utility value of critical infrastructure.

4. Critical infrastructure as a determinant of regional security

In security studies, "a region is a socially constructed category that historically emerges and disappears by connecting and separating geographical, political, economic, cultural and other units in one territory. Therefore, regions are not politically neutral, purely geographical categories, but are always social constructions, which arise on the basis of certain political power relations" (Ejdus, 2012). By building its unity in many areas, and especially its single market, the European Union has become the most important trade and investment partner, but also a source of development power towards the countries in its neighborhood (Dimitrijević, 2022). Exposed to various types of risks and threats in all security sectors, the Union had to plan its long-term actions in the field of security, with the active participation from all its members. In this context, the actions are primarily directed towards establishing a unified or at least harmonised normative framework. From the perspective of the importance of critical infrastructure for the security of the European Union, the characteristics of infrastructure elements such as complexity, interconnection and interdependence (Rehak, Senovsky, Hromada, & Lovecek, 2019), condition the common goals of the national security policy of the member states and the security of the European community.

The interdependence of critical infrastructure can be considered one of the main reasons for organising the protection of critical infrastructure at the regional level. Nevertheless, entities in the national security system are responsible for the organisation of the protection of critical infrastructure. When these subjects appear as bearers of activities and implementation of plans on the foreign policy level, as in the case of the protection of European critical infrastructures, they become part of the state's foreign policy system. The national normative framework regulating the field of critical infrastructure and its protection must not be in contradiction with European agreements, laws adopted by European institutions, agreements concluded by the European Union with third countries and international organisations, or the jurisprudence of the European Court of Justice. This means that the national security system of each country is determined by the international obligations accepted by the competent state

authorities, and the member states of the European Union should incorporate the protection of key entities of special European significance into their national security strategies.

The first official definition of European critical infrastructures was provided in Council Directive 2008/144/EC according to which '*European critical infrastructure*' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States" (Council Directive 2008/114/EC, 2008: Article 2 (b)). European critical infrastructures were supposed to be designated from national critical infrastructure, in accordance with national legislation and criteria for identification and designation of critical infrastructure. Consequently, the protection of European critical infrastructure was organised in accordance with the national legislation of the country where certain infrastructure of supranational importance is located (Sikimić, 2022c).

In principle, the directives do not prescribe mandatory instruments for achieving results, but prescribe the results that candidate countries must achieve. In 2018, an evaluation of the implementation of the guidelines of Council Directive 2008/114/EC was conducted, leading to the conclusion that 18 member states of the European Union adopted the proposals and requirements either by amending the existing or adopting new national legislation. In agreement with neighboring countries, 11 member states designated at least one European critical infrastructure. At the level of the European Union, 93 European critical infrastructures were designated, with 88 in the energy sector and 5 in the transport sector (European Commission, 2019). This outcome is one of the reasons why the Directive 2008/114/EC was repealed in 2022, and ongoing activities continue in accordance with the provisions of the Directive 2022/2557. According to Article 14 of the Directive 2022/2557, a critical entity of particular European importance provides essential services to more than one third of the Member States or in more than one third of the Member States of the European Union (Directive 2022/2557).

In addition to the member states of the European Union, candidate countries must ensure both national infrastructure and infrastructure and entities of importance for the European community (Sikimić, 2022c). Thus, the countries of the Western Balkans including the Republic of Serbia, Montenegro and the Republika Srpska (an entity in Bosnia and Herzegovina) adopted special laws to regulate the protection of critical infrastructure (Law on critical infrastructure, 2018; Law on Designation and Protection of Critical Infrastructure,

2019; Law on Critical Infrastructure Security in the Republika Srpska, 2019). Albania and North Macedonia are currently working on the development of such laws.

There are significant differences in the financial and institutional capacities of EU member states and non-EU member states regarding the establishment of security systems. In March 2022, the document "A Strategic Compass for the EU" was adopted, stating that the European Union will continue to provide financial assistance abroad within the objectives of the common security and defense policy. The assistance should be related to increasing defense capacities for crisis management, building additional civilian capacities, reforming the security sector, better governance and democratic supervision, compliance with the rule of law, human rights and international law (Council of the European Union, 2022; Dimitrijević, 2022). The political and security challenge for the entire region is the issue of Bosnia and Herzegovina, i.e. the ongoing problem of the division of competences between the state and the entities, which is also reflected in the area of critical infrastructure security, not normatively regulated in the entire territory of this country.

5. Threats and their consequences on critical infrastructure

According to the most general division based on the origin, i.e., the etiological dimension, we may talk about the following phenomena of threatening security: hazardous phenomena of natural origin, hazardous phenomena of human origin, hazardous phenomena of technical-technological origin and hazardous phenomena of combined origin (Mijalković & Popović, 2016). Operationalising this classification, and in the context of endangering critical infrastructure, the terms "incident" and "risk" are officially used. An incident represents any event that can disrupt or disrupts the operations of a critical entity, while a risk represents any circumstance or event that has a potential negative effect on security of critical infrastructure (Directive 2022/2557, Article 2).

In risk assessments for critical infrastructure, it is necessary to consider all relevant natural and human-induced risks, accidents, natural disasters, public health emergencies, hostile threats, including criminal acts of terrorism (Besenyő, Márton, and Shaffer, 2021). It is also essential to acknowledge all risks originating from other member states and third countries, and arising from the interdependence and interconnectedness of the infrastructure sectors (Directive 2022/2557, Article 4). More clearly, interruptions in the provision of essential services can result from natural disasters, errors within the infrastructure system and attacks on the critical infrastructure system (Nagy, Sikimić, & Baškalo, 2023). It is impossible to predict

and describe every type, form and type of natural disaster/climate change, system error or attack (Nagy, Boda, 2022). However, within the realm of modern security threats, cyber attacks are emphasised, as well as the risks associated by the (excessive) use of new technologies in all spheres of social life (Besenyő & Gulyás, 2021; Kovács & Besenyő, 2023; Amidzić & Sikimić, 2024). In addition, measures of political and/or economic coercion such as blockades, embargoes and boycotts may disrupt the provision of essential services.[3]

The consequences arising from interruptions in the operation of critical infrastructure include human losses, economic losses and the impact on the public. The continuity of the population, that is, the permanent settlement of people in a territory, is a condition for the existence of the state, so the possible number of fatalities or injured individuals is considered direct damage. The connection between critical infrastructure and consequences on human life and body can be found in different sectors.[4] Furthermore, critical infrastructure in the banking and finance sector encompasses the production of national currency, money distribution systems, insurance systems, banking operations, electronic banking and other services. The pillars of the national financial system are represented by the banks which play an important role in the economy of every country. Threats to the stock market, investments, payment systems and bank clients can lead to instability of the banking system and national currency. Finally, direct damage to critical infrastructure in the context of the public is assessed based on the impact on public trust, physical suffering and disruption of daily life, including the loss of essential and public services (Amidzić & Sikimić, 2024).

Long-term impact on the integrity of individuals and communities, long-term economic damage and long-term impact on the quality of the environment are also consequences of critical infrastructure insecurity. The fundamental human right is the right to life, and in addition, some human rights which simply and clearly illustrate the connection with the protection of critical infrastructure are: the right to health care, the right to social protection,

[3] The current military actions on the territory of Ukraine, which is not a member of the European Union, also have an impact on the member countries, their national, political, economic and security commitments. Although the military activities remained within the borders of Ukraine, the development of events affected the entire continent. The context of the energy crisis caused by the countries' significant dependence on Russian gas is the most well-known to the public. On the other hand, the lack of gas occurs as a result of a deliberate suspension, as European countries introduce extensive economic, trade and other sanctions against the Russian Federation.

[4] Lack of drinking water, food, thermal energy, etc. can lead to death. During the 2014 bombing, vital water and sewage infrastructure in Gaza was destroyed. Around 100,000 residents were left without water supply, and approximately 25,000 cubic meters of raw sewage were discharged into the sea daily. The damaged sewage infrastructure directly contributed to the spread of various stomach diseases and infectious illnesses such as jaundice. Similar infrastructural damage, waste accumulation and other issues occurred during the attacks in October 2023 (See more in: Buheji & Al-Muhannadi, 2023:33).

the privacy of correspondence and other means of communication, the protection of personal data, freedom of the media, the right to legal assistance, etc. If the health critical infrastructure is threatened (e.g. production, transport and supervision of medicines, inadequate vaccination and immunisation system), there is a disruption in providing health care to citizens and the health of the population is threatened (Sikimić, 2022b). Health security affects natural population growth, the fertility rate, the life expectancy, and consequently the fundamental human right - the right to life - is threatened. Attacks on information and communication infrastructure lead to violation of the rights to privacy of correspondence and other means of communication. Cyber attacks can also result in the public disclosure of protected personal data. If such situations persist or recur, there is a long-term impact on the integrity of the individual and the community.

One of the most significant problems of modern civilisation is the issue of the quality of drinking water. The consequences of "inadequate" drinking water often cannot be confined only to the population that consumes that water. Infectious diseases resulting from the use of contaminated water can reach epidemic proportions, thereby affecting even residents who use clean water. A precondition for people's health is agriculturally productive land, which provides higher quality and more affordable food with less energy consumption and artificial fertilizers, enabling the nutrition and sustenance of the population. The percentage of arable land is decreasing both due to erosions caused by human activities and those caused by natural processes (Sikimić, 2022b).

Telecommunication and information infrastructure constitute the infrastructure of all infrastructures инфраструктура (Kadena & Rajnai, 2024; Qose, Rajnai, & Fregan, 2023). The Internet, as a universal service, is one of the priority development goals of both national states and the European Union, and it is necessary to provide every individual with the access to the Internet at the individual level. The information society requires standardised network services, procedures and equipment, i.e. infrastructure conditions that will enable fast and secure data transmission. Information security is an integral component of national security and represents a cross-section of all security sectors where information technologies play a significant role. The main components of information security include the protection of personal data, state and official secrets, protection of data from accidental or intentional natural or artificial influences, guarantee of constitutional rights and freedoms of individuals and citizens regarding activities in the information sphere, and protection of citizens' needs from negative (intentional and accidental) information-psychological and information-technical influences. The digitisation

of data in public services poses a high degree of security risks. The weakest point in the electronic administration concept is the threat to critical information and telecommunication infrastructure, that is, security risks from potential cyber attacks, misuse and manipulation of databases. The methods, ways and means of criminal activities are becoming increasingly sophisticated and the use of information technologies increases the number of criminal acts in the credit and financial sphere and in the processing of personal data (Sikimić, 2022b; Amidzić & Sikimić, 2024).

The consequences of endangering critical information and telecommunication infrastructure can temporarily lead to the collapse of the country's health and education systems, as well as interruptions in the operation of the entire administrative apparatus. A significant part of the information resources is in private ownership, and precisely because of this, the dysfunctionality of the information systems of the non-governmental sector inevitably leads to the dysfunctionality of the information systems of the government sector. It is true that some countries do not have such a developed electronic business system, but the global confrontation with the COVID 2019 pandemic forced the entire planet to adapt and organise its entire life through information technologies (Sikimić, 2022b). Overnight, we become witnesses and actors in life "online".[5]

Although there is awareness of the importance of infrastructure, there is still no unified list or definition of critical infrastructure, which leads to different approaches to its protection. The critical infrastructure security policy is developed based on the identification and classification of infrastructure into vital sectors - by examining the most important characteristics of critical infrastructures and its essential services. The threat to only one sector of infrastructure can endanger the security of the social community, cause dysfunctionality of information systems in both governmental and non-governmental sectors, energy and economic instability and cause serious disruption in the free movement of people, transportation of goods and provision of services. The regional importance of critical infrastructure is conditioned by the interdependence and cascading effects of disturbances, but national security still plays a central role in protecting all other levels of security. Without the capacities and mechanisms of the national security system, it is not possible to achieve effective protection of infrastructures and entities that provide essential services across Europe, and the

[5] Adaptation to the "online" mode of teaching and taking exams was also represented in the doctoral studies, within which this dissertation was written.

leadership of the European Union has recognised the importance of international cooperation and joint response to incidents.

II. A CONTEMPORARY SECURITY FRAMEWORK FOR THE SECURITY OF CRITICAL INFRASTRUCTURES

1. Two decades of the European critical infrastructure protection policies path

The term *policy* covers the problem area and a complex of measures associated with it. Primarily, it implies the manner and process of decision-making, organising and implementing public activities, analysing and solving problems. It generally refers to activities conducted by the government, that is, the authorities, but this term also includes activities in the private sector (Ćeranić, 2020: 33).

The initiation of measures by the European community, in the identified problem area of critical infrastructure, began and took place under the influence of the terrorist attacks on the twin towers in 2001 (9/11), and another terrorist attacks in Madrid (2004) and London (2005). From the very beginning, the mission of the European approach was to provide an adequate level of protection for all critical infrastructures, especially for those whose disruption would have a significant impact on the social life and security of a member state (Lazari, 2014: 46). In 2004, the European Council requested the European Commission to prepare a strategy for the protection of critical infrastructures. In response to this request, a proposal was developed to jointly strengthen the system for the protecting critical infrastructures in Europe, in the form of the document *Critical Infrastructure Protection in the Fight Against Terrorism* (European Commission, 2004). During the following year, seminars on the protection of critical infrastructure were organised, with the aim of involving the main actors and the private sector. At these seminars, member countries shared their national experiences on determining the scope of action and the stakeholders involved in the protection of critical infrastructure. In this way, awareness was raised among private sector entities about the importance of joint efforts (Lazari, 2014: 45). The mentioned activities led to the sublimation of the results in the document *Green Paper on a European Programme for Critical Infrastructure Protection* (European Commission, 2005).

Further work on the development of policy for the protection of European critical infrastructures was based on the inclusion of as many stakeholders as possible and the establishment of a common program for the protection of critical infrastructures. Some of the elements on the basis of which a common framework for the protection of critical infrastructures was to be formed included unique principles for protecting critical infrastructure, unique standards, unique criteria for determining critical infrastructure, a unique

list of critical infrastructure sectors, a description of the obligations of responsible entities as well as methodologies for determining critical infrastructures in different sectors (European Commission, 2005).

In December 2008, a document was adopted which defined the purpose, principles and content of the European program *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*. This document describes a multi-stage procedure in which the primary and ultimate responsibility for the protection of national and European critical infrastructures rests with member states and owners/operators of critical infrastructures (Sikimić & Gnjatović, 2020). Member States were instructed to implement the guidelines from the Directive 2008/114/EC into their national legislation within a two-year period.

The intention of the creators was to enable, or rather impose a common model or the so-called "European benchmark" for the identification and designation of European critical infrastructures through the adoptiion of the Directive 2008/114/EC. The mentioned procedure was based on a "bottom-up" approach, meaning that the final decision on the designation of European national critical infrastructure was within the competence of the member state on whose territory the specific infrastructure is located. Furthermore, the European Commission could only be involved in the process of identification and designation if the member state requested assistance (Council Directive 2008/114/EC).[6] According to Lazari, in this designed path it meant that the European Commission plays the role of a "facilitator" in the implementation of the public policy for the protection of critical infrastructures (CIP policy), while the principle of subsidiarity assigns the primary and ultimate responsibility for the protection of critical infrastructures to the member states. Finally, with the Directive 2008/114/EC the first (initial) step was taken and a *step-by-step* procedure for the identification and designation of European critical infrastructures was established (Lazari, 2014: 48-51).

States protected their vital facilities, systems and networks in some way even before the adoption of the Directive 2008/114/EC. Bearing this fact in mind, the Directive 2008/114/EC leaves room for such measures to remain in force, providing that they do not contradict the European program. Existing measures can even serve as an example of best practices when implementing the Directive 2008/114/EC into national legislation. The plan

[6] Although a "top-down" approach was designed in the Green Paper, which envisages that the European Commission has full control when designating European critical infrastructures, the Directive completely replaced this approach with a "bottom-up" approach.

was also to avoid duplication of regulations, so the Directive 2008/114/EC did not necessarily require the adoption of new regulations or changes if they already existed, or consolidation with the envisioned European program for the protection of critical infrastructures could be achieved through changes and/or amendments (Council Directive 2008/114/EC).[7] Simply put, the purpose of all programs and measures for the protection of critical infrastructure was to enhance the protection of important facilities with the aim of enabling and improving the safety of people in general. Although, based on the given guidelines, it might seem that the focus of the Directive provisions was on "how", the emphasis was primarily on the results to be achieved (Sikimić, 2022c). Lazari states that in that process, the Directive 2008/114/EC was only an "additional layer" meant to upgrade the national frameworks for the protection of critical infrastructure (Lazari, 2014: 52). Thus, the states had different approaches such as: "Amendments to existing laws and regulations (four Member States); New Laws (eight Member States); Resolutions (four Member States); Procedural changes to existing critical infrastructure protection related activities (two Member States and United Kingdom); Decrees and Executive orders (eight Member States)" (Lazari, 2014: 73-75). Additionally, four new national laws on critical infrastructure were adopted in the Western Balkans (Sikimić, 2022c).

In the development of the envisioned public policy for the protection of critical infrastructure, several challenges emerged, among which are: political context, national interests, differences in national legislation, geographical location of the country, conflicts, social status, emphasis on terrorism as the main threat,[8] and the imposed two-year timeframe.[9] Confronting the mentioned challenges has often resulted in the non-designation of European critical infrastructures.

Political will has sometimes accelerated,[10] and sometimes hindered the process of legislative upgrade due to national interests focused on different types of threats against which that country has already developed an action plan. Depending on societal awareness of the existence of a threat or how individual countries assess risks, the application of cross cutting criteria did not lead to the identification of any European critical infrastructure. The geographical position directly conditioned the designation of the critical infrastructure sector,

[7] Thus, France had its own decree since 2006, which significantly consisted of a translation of the provisions of the Directive (Decret no 2006-212 du 23 fevrier 2006 relatif a` la securite´ des activites d'importance vitale, 2006).
[8] Although the Directive proclaims comprehensive protection against all types of risks and threats, it primarily emphasises the protection against terrorist threats (Council Directive 2008/114/EC).
[9] The member states were obliged to create a list of European critical infrastructures which would be continuously updated within two years from the date of entry into force of Directive 2008/114/EC.
[10] In the context of terrorism, there was generally no lack of promptness on the part of political actors.

as it is necessary to organise the security system differently in countries surrounded by mountains (landlocked) than those with the access to the sea and kilometers of coastline. The geographical location directly affects the type of transport prevalent in an area, as well as variables in the energy sector.

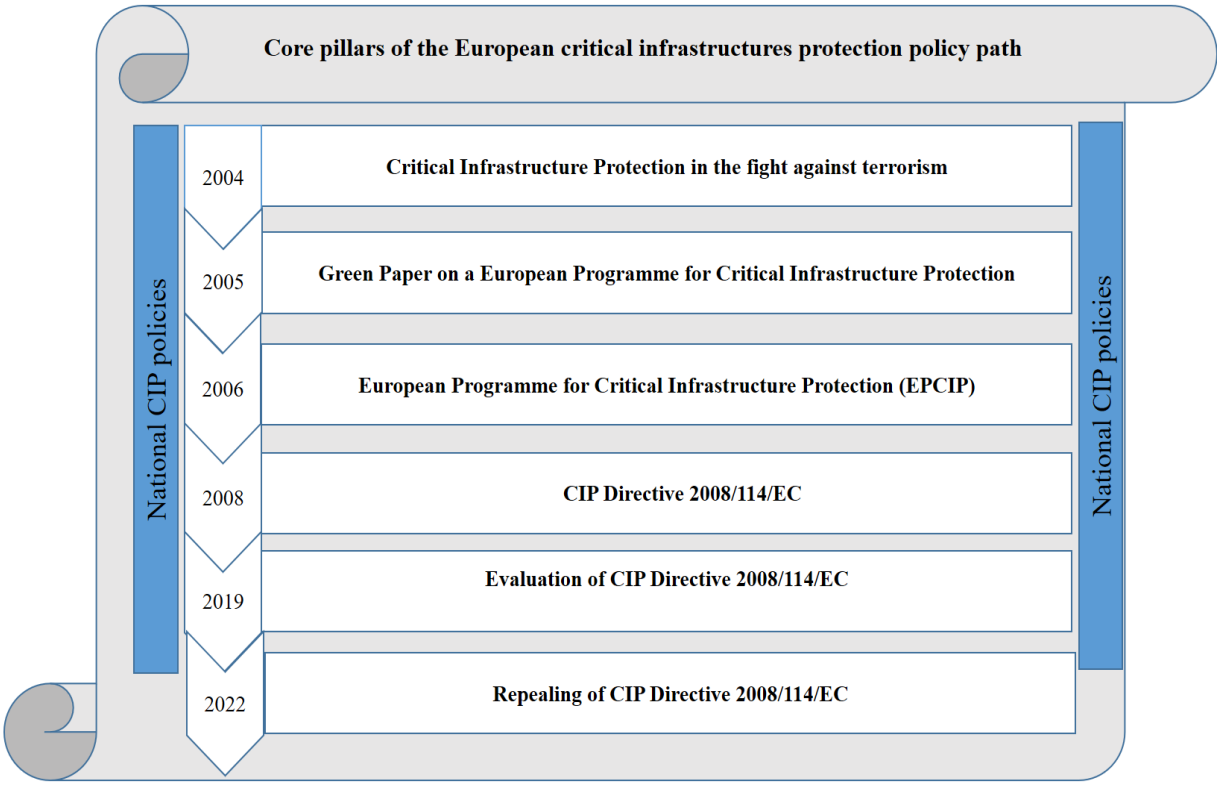


Figure 2.1: Development of the European critical infrastructure protection policy[11]

Regulating a broad area like critical infrastructure is not easy at the national level, and harmonising at the level of the European community is certainly even more difficult. One of the challenges faced by the actors is that it is not easy to work on uniformity in the wide range of available alternatives. Conflicts are part of the Europe's historical heritage and also its present. Therefore, sharing of information about critical infrastructure, or honesty in bilateral relations is certainly not something that national actors, as well as the European Commission can reliably count on as entities of public policy for the protection of critical infrastructure. Additionally, the development of technologies, the establishment of research centers,

[11] Source: creation of the author, based on the results obtained from the content analysis.

experimental capacities and ultimately the implementation of measures for the protection of critical infrastructure directly depend on the economic development of the state.

Evaluation criteria	Evaluation findings: the directive ...	Comments
Relevance	remains partially relevant	• The context and nature of threats have changed since the directive was adopted. • The sectoral approach taken is outdated. • The focus is on protection, whereas resilience is just as important.
Coherence	is broadly consistent with relevant sectoral legislation	• There are complementarities and certain overlaps, especially with the NIS Directive. • More could be done to exploit synergies. • There is coherence with international initiatives.
Effectiveness	is partially effective in achieving its objectives	• The procedure of identification and designation is not fully aligned across Member States. • **The evaluation results as to whether the directive has raised the level of protection of ECIs are inconclusive.**
Efficiency	*no conclusive evidence*	• *lack of quantifiable data*
EU added value	has EU added value	• Results could not have been achieved at national level. • Political momentum was created on CIP. • Cross-border dialogue and cooperation between Member States was encouraged.
Sustainability	has long-lasting effects	• Certain elements/structures would continue to exist even if the directive were to be repealed.

Table 2.1: Conclusions of the evaluation in the light of the 'better regulation' criteria[12]

The revision of what was done according to the Directive 2008/114/EC began in 2017, and the document was published in 2019. The evaluation process was based on several criteria: Relevance, Coherence, Effectiveness, Efficiency, EU added value and Sustainability. The results showed that the Directive 2008/114/EC is still partially relevant and partially effective in achieving its goal. There were comments that the sectoral approach is outdated, that the focus must be placed on the resilience of critical infrastructures in addition to its protection considering the changed context and the nature of security threats, and that the identification

[12] Source: European critical infrastructure Revision of Directive 2008/114/EC, p 7. (Anglmayer, 2021).

and designation procedure is not harmonised in the member states. The Directive 2008/114/EC was mostly harmonised in the sector approach, but there were no relevant results regarding the possible increase in the level of protection of European critical infrastructures. However, the Directive 2008/114/EC has stimulated political momentum in regional security through cross-border dialogue and cooperation among member states in the field of critical infrastructure protection. This has led to long-term effects and elements of European security that will persist even after the repeal of the Directive 2008/114/EC (Anglmayer, 2021).

The described results have led to the need for the expansion of the existing actions, which was done by adopting a new proposal that relies on the lessons learned from the Directive 2008/114/EC, but also repeals the Directive 2008/114/EC. This proposal is one of the building blocks of the new EU Security Union Strategy for 2020-2025, which emphasises the importance of ensuring the resilience of critical infrastructure in the face of physical and digital risks.

2. The Directive (EU) 2022/2557 on the resilience of critical entities

Some of the reasons and objectives for the adoption of Directive (EU) 2022/2557 of the European Parliament and the Council of December 14, 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC are contained in the amended corpus of security challenges, risks and threats. The security environment in the third decade of the 21st century is characterised by hybrid activities, new technologies such as 5G, drones and artificial intelligence. There are also pandemics, industrial accidents, natural disasters often exacerbated by climate change, terrorism and internal threats. One of the key challenges for operators is to face the advancement of their business by implementing new technologies, while protecting against new security risks brought by these technologies. Thus, basic services that are an integral part of everyday life are usually provided by closely interconnected networks of companies. Disruption in one sector can have a cascading effect and hinder the provision of services in other sectors, member states or the entire European Union. The member states have taken their own measures in the field of cybersecurity and civil protection, and the aim of the Directive 2022/2557 is to establish a new common approach (Directive 2022/2557, 2022).

As explained on the previous pages, the Directive 2008/114/EC was created and developed under the pressures of terrorist attacks in New York, Madrid and London. However, the proposal for the Directive 2022/2557 was submitted during the period of the energy crisis

in Europe and the damage to the "Nord Stream" gas pipeline.[13] Therefore, it is not surprising that preparedness, response and international cooperation are prioritised in the critical infrastructure of the energy sector. Some of the targeted actions of the new approach presented in the Directive 2022/2557, to which the European Commission invites member states, include updating risk assessments, testing critical entities and developing a plan for the coordinated response to disruptions in critical infrastructure with cross-border significance from a range of threats, including natural hazards, terrorist attacks, insider threats or sabotage. Finally, the Council approved the Directive 2022/2557 on December 8, 2022 with a recommendation which aims to reduce the vulnerabilities and strengthen the resilience of critical entities. Member states are obliged to implement the requirements from the Directive 2022/2557 into national legislation by October 17, 2024, and these measures should be applied starting from October 18, 2024. The general goal is for operators, i.e. critical entities, to be resilient, which means that they must be well protected and capable of restarting their business in the shortest possible time in the event of a disruption. By January 17, 2026, each member state should adopt a national strategy for enhancing the resilience of critical entities.

2.1. Determinants of national frameworks for the resilience of critical entities

The subject of the Directive 2022/2557 is to impose obligations on member states to ensure the uninterrupted provision of services, that is, to identify critical entities and enable them to enhance their resilience and delivery of essential services. It also mandates supervision during the execution of obligations with an emphasis on critical entities considered to be of particular European significance (Directive 2022/2557, Article 1).

The obligation of the member states is to establish strategic goals and policy measures in order to achieve and maintain a high level of resilience of critical entities, that is, to develop a strategy for strengthening the resilience of critical entities. The strategy should minimally indicate the following:

- strategic goals and priorities for the purpose of strengthening the resilience of critical entities,
- management framework for achieving the set goals,
- a description of the measures needed to strengthen the resilience of critical entities and

[13] Damage to the "Nord Stream" gas pipeline was characterised as sabotage and "unacceptable deliberate disruption of the European energy infrastructure" by Ursula von der Leyen, head of the European Commission.

- the framework of public policy for coordination and exchange of information, with an emphasis on joint information security (Directive 2022/2557, Article 3).

When defining strategic goals and priorities, it is necessary to consider the cross-border and cross-sectoral interdependence of critical entities, while the management framework should contain a description of the roles and responsibilities of different bodies, critical entities and other stakeholders involved in the implementation of the strategy. Mandatory measures include a national risk assessment, identification of critical entities and entities equivalent to critical entities, and measures to support critical entities (Directive 2022/2557, Article 3).

Each member state appoints one or more competent authorities responsible for implementing the Directive 2022/2557 into national legislation and effectively enforcing its provisions in practice. In the case of appointing several such authorities, it is necessary to clearly establish the relationships between these bodies and establish effective cooperation.

Within one of the responsible entities, a single point of contact is established, performing the function of connecting and facilitating international cooperation with a point of contact of other countries and with the Critical Entities Resilience Group. The state is obliged to provide the authority performing the function of a single point of contact with material, personnel and technical conditions for work. After the countries have submitted information on the designated competent authorities and single points of contact, the European Commission will publish a list of the single points of contact of the member states (Directive 2022/2557, Article 8).

The Directive 2022/2557 determines 11 sectors in which member states are required to conduct regular risk assessments and identify entities that are considered critical or vital for society and the economy. These sectors are:

- energy,
- transport,
- banking,
- financial market infrastructures,
- health,
- drinking water,
- wastewater,
- digital infrastructure,
- public administration,

- space and
- food.

In order to determine critical entities, competent authorities create a list of services within sectors and conduct an assessment of all relevant risks that may affect the provision of essential services. “Risk assessment means a methodology to determine the nature and extent of a risk by analysing potential threats and hazards and evaluating existing conditions of vulnerability that could disrupt the operations of the critical entity” (Directive 2022/2557, Article 2). General and specific risk assessments are considered, including risks arising from cross-sectoral and cross-border dependencies encompassing third countries, all information on reported incidents, and in general risks of natural and human origin, accidents, natural disasters, public health emergencies and hostile threats including terrorism (Directive 2022/2557, Article 4). Relevant elements and results of the risk assessment must be accessible to critical entities and the European Commission.

Based on the results obtained in the risk assessments, the member states identify critical entities in each of the sectors and sub-sectors and compile a list of critical entities. After determining the critical entities, the state has to inform them of their obligations and the date when the provisions of the Directive 2022/2557 apply to them. If a certain entity is identified as critical in two or more countries, further work is done on consultations between these countries in order to reduce the burden on that subject.

The Directive envisions a situation where it is determined how a certain entity provides services to more than one third of the member states or in more than one third of the member states. In that case, it is necessary to immediately inform the European Commission about the identity of that/those critical entities.

Additionally, the lists of critical enities are updated as necessary, at least every four years (Directive 2022/2557, Article 5). Within the banking sector, financial market infrastructure and digital infrastructure, there is the possibility of designating entities equivalent to critical entities, which will be considered critical entities only for the purposes of establishing national frameworks for the resilience of critical entities (Directive 2022/2557, Article 3-7).

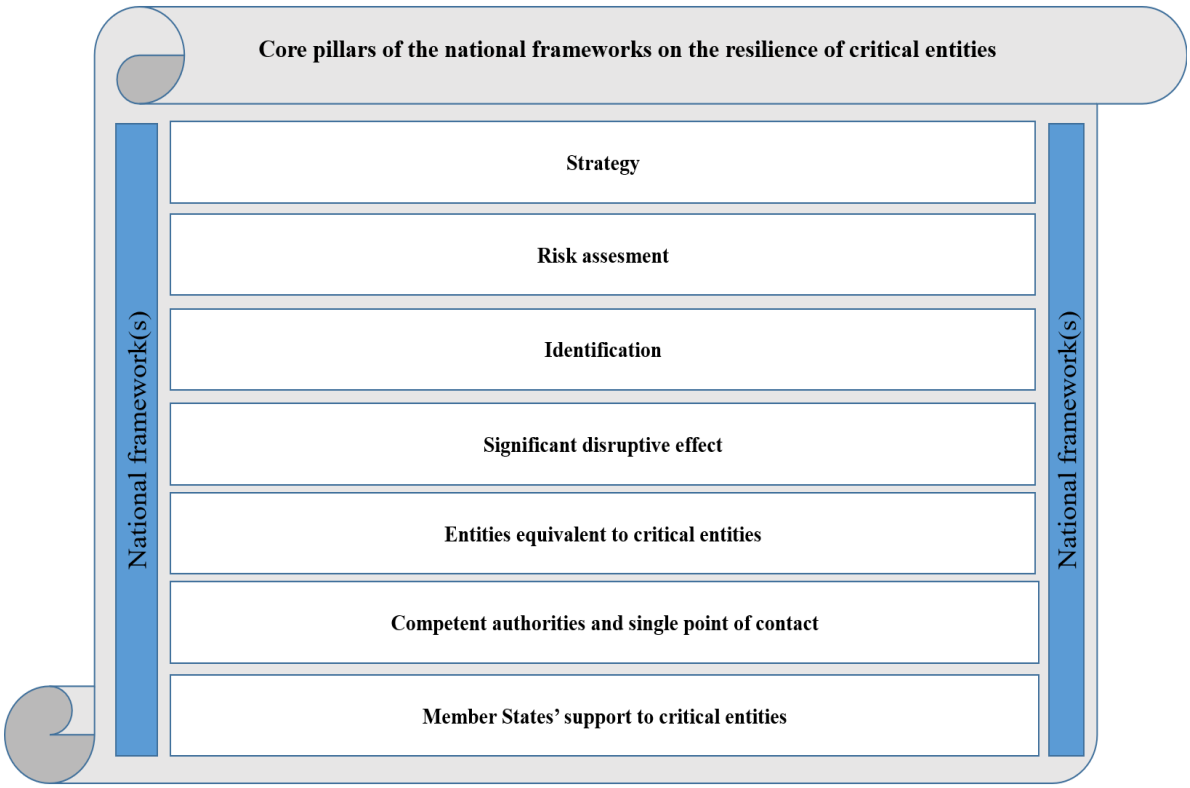


Figure 2.2: The core national pillars of the contemporary European security framework[14]

In addition to identifying critical entities and compiling a unique list of critical entities, responsible bodies at the national level also compile a list of essential services provided by critical entities in all sectors and subsectors, and determine the so-called significant negative effects in case of disruption or interruption in the provision of the identified essential services. When determining the negative effects, the number of users whose functioning requires one or more services provided by a certain critical entity is considered, as well as the availability of alternative ways to provide that service. It is also necessary to determine the geographical area where the influence could be manifested, including the territories of other countries. Another important criterion is dependence, i.e. the impact that could be felt in other sectors, as well as the degree and duration of negative effects that incidents could have on public safety, state and social activities (Directive 2022/2557, Articles 4-8).

Member States undertake to provide critical entities with all necessary support in order to provide uninterrupted delivery of essential services and strengthen their resilience. The provisions of the Directive in this case are quite broadly framed, which leaves the possibility of a wide range of measures and actions, which will depend and vary from country to country.

[14] Source: Author's creation.

Thus, support may include training of personnel employed in a critical entity, organising exercises and testing the resilience of a critical entity, developing guidelines and methodologies that can be used to raise the level of resilience, etc. The support also encompasses the exchange of information, good practices and cooperation at both intersectoral and interstate level (Directive 2022/2557, Article 9).

2.2. Measures for the resilience of critical entities and competent authorities

After the state conducts a risk assessment, identifies critical entities and informs them about it, each critical entity is obliged, within its jurisdiction, the scope of work and the provision of services, to assess all relevant risks that may disrupt its operations. The state supervises through the competent authorities the implementation of appropriate organisational and technical measures by the critical subject. One of the obligations of critical entities is to prepare a resilience plan or a similar document that will contain a resilience plan outlining detailed measures. Article 11 of the Directive prescribes the following measures as mandatory:

- prevention of incidents,
- appropriate physical protection,
- mitigation and reduction of consequences,
- recovery,
- adequate security management and raising the awareness of employees about the importance of the mentioned measures (Directive 2022/2557, Article 11).

When planning and implementing measures to prevent the occurrence of incidents, it is necessary to consider methodologies for reducing the risk of disasters, as well as guidelines for adapting to climate change.

Adequate physical protection of sensitive areas, facilities and other infrastructure implies the installation of fences, partitions, various tools and routine procedures for area surveillance, detection and access control. Recovery measures refer to taking measures for the purpose of maintaining business continuity and identifying alternative supply chains, while an integral part of measures for mitigating consequences are procedures for managing risks in emergency situations (Directive 2022/2557, Article 11).

Security management refers to identifying categories of personnel performing critical functions. It is necessary to control access to sensitive areas and sensitive information in accordance with the authorisations of individual employees. In this part, it is envisaged that critical entities will be able to submit requests for background checks of individuals among the

staff assigned to specific jobs and tasks. It is about the so-called special categories of persons who are employed or apply for employment in sensitive and important positions within the critical entity. States are required to regulate with their legislation that security and other authorised entities conducting checks are obliged to carry out checks and deliver information to the critical entity that submitted the request in an urgent manner. Such checks encompass the following:

- determining the identity of the person,
- verifying previous employment and education, including any interruptions in education or employment in at least the previous five to a maximum of ten years,
- obtaining criminal records on criminal offenses relevant to employment, for the above-mentioned time period (Directive 2022/2557, Article 12).

Regarding the geographical factor, the checks include all criminal offenses relevant to employment in a certain position in the critical entity, which were committed on the territory of a member state, in another member state whose citizenship the person holds, as well as in all member states or third countries where the person stayed during the period covered by the checks. The Directive 2022/2557 requires member states to mutually exchange requests for criminal records checks and provide responses within ten days. The possibility of extended checks is foreseen, which implies the use of intelligence data and "any other objective information available that may be necessary to determining the suitability of the person concerned to work in the position in relation to which the critical entity has requested an extended background check" (Directive 2022/2557, Article 12).

Within the chapter on the resilience of critical entities, there are provisions of the Directive 2022/2557 that refer to the mandatory reporting of an incident that has already occurred or an incident that may occur in the near future and significantly disrupt the operations of a critical entity. The critical entities inform the competent state authority without delay about the nature, cause and possible consequences of the incident. This information should also include elements such as the number of users affected by the disruption or potential disruption, the duration or expected duration of the disruption, and the geographic area where the effects of the disruption may be felt. On the basis of the received information, the state authority forwards the data to the points of contact of other states through a single point of contact. This occurs if the reported incident may have or has already had a cross-border impact in any of the countries, and the information is communicated only to those countries (Directive 2022/2557, Article 13).

The described communication is two-way, because the competent state authority submits a response to the notification received from the critical entity. The response contains instructions on the further actions of the critical entity, that is, all possible support is provided to the critical entity in order to contribute to the effective prevention or suppression of the incident.

A special form of supervision is provided for those entities that provide essential services to more than one third of the member states or in more than one third of the member states, i.e. critical entities of special European importance. While for national critical entities, the supervision of the implementation and the implementation of security measures is organised by the competent state authority, in the case of critical entities of special European importance, the European Commission conducts advisory missions to assess the measures taken by that entity. The members of the advisory missions are experts from member countries selected and appointed by the European Commission at the suggestion of the state, based on their expertise. In addition to the representatives of the member states whose geographical diversity is taken into account, the members of the advisory missions are also representatives of the European Commission, and the work of these missions is directly financed by the European Commission. The European Commission also adopts a program according to which the advisory missions will operate. However, the minimum or maximum duration of the advisory mission is not specified (Directive 2022/2557, Article 15).

Advisory missions are obliged to respect the national legislation of the country where the mission is conducted, that is, where the subject infrastructure is located. On the other hand, the member state hosting the subject of the advisory mission is required to provide unhindered access to all information, systems and facilities related to the provision of services of a critical entity of special European importance.

The findings of the advisory mission are submitted to the Critical Entities Resilience Group and the European Commission within three months after the conclusion of the mission. Further, additional measures to enhance the resilience of the specific entity may be imposed, and special expertise on disaster risk management may be requested from responsible individuals within the critical entity (Directive 2022/2557, Article 15). This part is mediated by the Emergency Response Coordination Centre.[15]

[15] The Emergency Response Coordination Centre (ERCC) is the EU Civil Protection Mechanism. It coordinates the delivery of assistance to disaster-stricken countries, such as relief items, expertise, civil protection teams and specialised equipment and acts as a coordination hub between all EU Member States, the 10 additional

The assessment of national strategies for the resilience of critical entities is the task of the Critical Entities Resilience Group. It is envisaged that this body will be formed within six months of the entry into force of the Directive 2022/2557 with the task of facilitating strategic cooperation and information exchange. The members of the Critical Entities Resilience Group are representatives of the member countries and representatives of the European Commission, with the possibility of inviting membership from any potentially necessary and/or interested third parties. The main task of the Group is to support the European Commission in providing assistance to the member countries in the development of national strategies for the resilience of critical entities, evaluating strategies and finding best practices in relation to strategies in order to facilitate the exchange of experiences on measures implemented by different countries (Directive 2022/2557, Article 16). It can be said that this body has the role of an instructor, but also a controller over the member states. On an annual basis, the Group conducts reviews of reports on the exchange of information that single national points of contact are required to submit. Additionally, the Group is obliged to adopt its work program every two years, and meet at least once a year with the cooperation group established in accordance with acts on cybersecurity (Directive 2022/2557, Articles 8 and 16).

The Commission shall complement member states' activities in enhancing their resilience by developing best practices and methodologies, and by developing cross-border training activities and exercises to test the resilience of critical entities (Directive 2022/2557, Article 17).

2.3. Implementation and supervision

Within 18 months from the entry into force of the Directive 2022/2557, the member states must transpose the requirements of the Directive into national law, and apply them after the expiry of the two-year period plus one day. Furthermore, by the middle of 2027 ("by 54 months after the entry into force of this Directive"), the European Commission must submit a report to the European Parliament on the state and level of measures taken by the member states to comply with the Directive 2022/2557 (Directive 2022/2557, Articles 22-24).

participating states (namely: Albania, Bosnia and Herzegovina, Iceland, Moldova, Montenegro, North Macedonia, Norway, Serbia, Turkey and Ukraine), the affected country, and civil protection and humanitarian experts. The ERCC operates 24/7. It can help any country inside or outside the EU affected by a major disaster upon request from the national authorities or a UN body. The centre ensures cooperation and coherence of EU action at an inter-institutional level, focusing on coordination mechanisms with the European External Action Service, the Council and EU Member States.

Competent state authorities are empowered to request information from critical entities necessary to assess whether the measures taken by that entity are in accordance with the measures prescribed by the Directive 2022/2557 and/or the national legislation enacted on the basis of this Directive, as well as evidence of the effective implementation of those measures. In other words, the competent state authority conducts direct supervision of space used by critical entities, as well as indirect supervision of resilience measures undertaken by critical entities. If a non-compliance or an insufficient level of measures taken by the critical entity is determined, the competent authority may impose a reasonable deadline for the critical entities to eliminate all identified deficiencies within and submit a report on it. Potential sanctions are stipulated through the national legislation of each country (Directive 2022/2557, Articles 18-19).

3. Cybersecurity

In accordance with the Directive 2022/2557, designated critical entities are subject to the provisions of *Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022 on measures for a high common level of cybersecurity across the Union* (NIS2 Directive)[16] and in this part of the dissertation we will discuss certain provisions of the NIS2 Directive related to critical entities. Directive 2022/2557 and NIS2 Directive were adopted on the same day and refer to each other, i.e. they are interconnected (NIS2 Directive, Article 2 (3)).

With the ultimate goal of improving the functioning of the internal market of the European Union, the NIS2 Directive establishes measures to achieve a high level of common information security. The steps that member states are required to take in terms of information security refer to the obligation to:

- adopt a national strategy on information security,
- appoint competent authorities,
- appoint authorities for information crisis management,
- establish a single point of contact for information security and
- form CSIRT - Computer security incident response team.

National cybersecurity strategy means a "coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to

[16] Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

achieve them in that Member State" (NIS2 Directive, Article 6(4)). In addition to measures for information security risk management mandatory for all critical entities designated in accordance with the Directive 2022/2557, the NIS2 Directive prescribes sectors of high criticality within which the entities of high criticality will be designated, and the provisions of this directive will be obligatory for them. These sectors include:

- energy,
- transport,
- banking,
- financial market infrastructures,
- health,
- drinking water,
- waste water,
- digital infrastructure,
- information and communication technologies service management,
- public administration and
- space (NIS2 Directive, Annex I).

Within these sectors, several sub-sectors have been designated, as well as "other critical sectors", among which are postal and courier services, waste management, manufacture, production and distribution of chemicals, production, processing and distribution of food, manufacturing (of medical, electronic, optical products, electrical equipment, motor vehicles, trailers and semi-trailers and other transport equipment), digital providers and research (research organisations) (NIS2 Directive, Annex II).

The NIS2 Directive applies to medium-sized enterprises and those exceeding the threshold for medium-sized enterprises, that provide their services or perform activities within the European Union.[17] However, the size of the company will not be taken into account if the entities provide services in the field of public communication networks or publicly available communication services, confidential services, top-level domain name registries and domain name system service providers. The same applies if the entity in a country is the only provider of a service that is crucial for the functioning of the state and society, if a disruption in the provision of services by a certain entity could significantly impact public safety and health and

[17] Medium-sized enterprises are considered to be those organisations that have less than 250 employees and an annual turnover of up to 50 million euros, that is, a total annual balance of up to 43 million euros. For comparison, small businesses operate with less than 50 employees and an annual turnover of up to 10 million euros (Official Journal of the European Union L 124/36, Annex I, Article 2).

cause major systemic risks with a cross-border effect. In accordance with this Directive information security measures must also be conducted by entities which are crucial due to their specific role at the national or regional level, by the public administration entities at the national or regional level, and by all critical entities providing domain registration services (NIS2 Directive, Article 2 (1-4)). It is possible to make an exemption in relation to public administration entities that perform activities in the area of national security, public security, defense or internal affairs, which also implies an exemption from the obligation to provide information whose disclosure would be in conflict with the interests of national security (NIS2 Directive, Article 2 (7-11)). Finally, by April 17, 2025, the member states should establish a list of essential and important entities, and entities that provide domain name registration services, and then regularly and, at least every two years, check and update the list (NIS2 Directive, Article 3(3)).

Competent authorities, which are appointed by each member state, are responsible for monitoring the implementation of national strategies. The state has the right to appoint one or more competent authorities, but in any case it must establish a single point of contact. If only one competent authority is appointed, then it serves as a single point of contact that achieves communication and cooperation with equivalent points of contact in other countries, as well as cross-sectoral cooperation with other competent authorities in its country. This body communicates with the European Commission and the European Union Agency for Cybersecurity (ENISA) as necessary. The member states are obliged to provide the European Commission with the identification data of the authority that is their single point of contact, after which the Commission consolidates the data and publicly publishes the list of single points of contact of all countries (NIS2 Directive, Article 8). With the competent authorities established under the provisions of the NIS2 Directive, information is exchanged by the competent authorities appointed on the basis of the Directive 2022/2557. Competent state authorities exchange information on cybersecurity threats, risks, incidents outside the information space, affecting key entities that have been identified as critical entities, as well as on measures taken and responses to risks, threats and incidents (NIS2 Directive, Article 13).

All critical entities (according to the Directive 2022/2557) are also key entities (according to the NIS2 Directive), while key entities do not have to be critical entities.

Articles 9 and 10 regulate the competencies and obligations of competent authorities responsible for managing large-scale information security incidents and computer security incident response teams. It is important to state that the provisions of the NIS2 Directive give

the possibility to CSIRTs to cooperate and exchange relevant information with teams of third countries, including the exchange of personal data (NIS2 Directive, Articles 9 and 10). In order to facilitate more efficient exchange of information between countries, enhance strategic cooperation and strengthen trust, the establishment of the Cooperation Group is mandated. This group consists of representatives of the member states, the European Commission and the European Union Agency for Cybersecurity (ENISA). In addition to the basic obligations prescribed in Article 14 of the NIS2 Directive, the Cooperation Group meets at least once a year and exchanges information with the Critical Entities Resilience Group (Directive 2022/2557, Article 16 and NIS2 Directive, Article 14).

Finally, the competent authorities from the NIS2 Directive provide information on incidents, cyber threats and avoided incidents to the competent authorities from Directive 2022/2557.

4. Data protection

Protection of data and information in the context of critical infrastructure security is considered from two aspects. One aspect relates to the protection of personal data of individuals who come or may come into contact with sensitive information about critical infrastructure and operations of critical entities, while the other aspect relates to the security of confidential information that protects the critical entity and/or its commercial interest.

Possibilities for checking the suitability of individuals belonging to certain special categories of personnel in the critical entity were established through the *Framework Decision of the Council 2009/315/PUP on the organisation and content of the exchange of data from criminal records between member states* (Official Journal of the European Union L 93/23, 2009) and *Regulation (EU) 2019/816 of the European Parliament and of the Council* (Official Journal of the European Union L 93, 2009 and L 135, 2019).[18] In addition, checks are conducted in compliance with the *General Data Protection Regulation*[19] and national legislation.

[18] Regulation (EU) 2019/816 of the European Parliament and of the Council of April 17, 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, Official Journal of the European Union L 135.

[19] European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/ EC (General Data Protection Regulation - GDPR), Official Journal of the European Union L 119.

Framework Decision of the Council 2009/315/PUP refers to judicial cooperation in the European Union. More specifically, it regulates the rules on the protection of personal data from convictions that are transmitted between member states. The primary objective of this decision is to define the ways in which a member state, which has handed down a conviction against a national of another member state, transmits the information on such a conviction to the member state of the convicted person's nationality. In addition, obligations to store data and reply to a request for information extracted from criminal records are defined, as well as a computerised system of exchange of information on convictions (Official Journal of the European Union L 93, Article 1). "The main aim of establishment of criminal records is to inform the authorities responsible for the criminal justice system of the background of a person subject to legal proceedings with a view to adapting the decision to be taken to the individual situation… The use of information transmitted under this Framework Decision for purposes other than that of criminal proceedings can be limited in accordance with the national law of the requested Member State and the requesting Member State" (Official Journal of the European Union, L 93/23). Regulation (EU) 2019/816 enables the above-described data exchange to take place with third countries (non-Member States), and includes citizens of the European Union who have the citizenship of a third country. In fact, Regulation (EU) 2019/816 designates "a system to identify the Member States holding information on previous convictions of third-country nationals (ECRIS-TCN)" (Official Journal of the European Union, L135, Article 1). The provisions of this regulation also determine the conditions under which EUROJUST, EUROPOL and EPPO use the system, and they also apply to the processing of identity information on citizens of third countries (Official Journal of the European Union, L135). However, the information stored in the criminal records are in the form prescribed by the national legislation of each country.

Nevertheless, the protection of individuals in the context of personal information processing is a fundamental right. The General Data Protection Regulation (GDPR) was launched on May 25, 2016, with its provisions coming into force directly in all Member States two years after, on May 25, 2018. The GDPR brings harmonised, directly binding data protection laws across the European Union. From the point of view of its territorial scope, the main purpose of the GDPR is to protect rights and freedom of natural persons from the European Union related to collection and processing of personal data, but the GDPR is also applied to third countries in situations when personal data of entities from the European Union are processed (Sikimić, 2022a). The GDPR applies to the processing of personal data in the context of the establishment of controllers or processors in the European Union, regardless of

whether the processing takes place in the European Union or not (GDPR, 2016). Also, it applies to the processing of personal data of data subjects who are in the European Union by controllers or processors not established in the European Union, where the processing activities relate to 1) the supply of goods or services, irrespective of whether the payment of the data subject is required, to such data subjects in the European Union or 2) monitoring their behaviour providing that it takes place within the European Union (Midorović & Sekulić, 2019). However, the GDPR does not apply to the processing of personal data by competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or enforcing criminal sanctions, including protection against threats to public safety (Official Journal of the European Union L 119).

Another aspect of data protection that is discussed concerns the protection of sensitive/confidential information about critical entities. The Directive 2022/2557 and NIS2 directives require the exchange of important information, but also provide for an exemption from the exchange with other countries of information directly related to the preservation of national security, such as information on public administration bodies designated as critical entities, military and police facilities and operations, etc. The degree of confidentiality and protection of such information is governed by the national legislation of each country.

Critical infrastructure protection has been characterised by different national approaches, and an attempt to introduce a uniform security framework in the European Union was presented through Directive 2008/114/EC in 2008. The implementation of the envisioned model based on the sectoral approach has facilitated the development of regional cooperation and cross-border dialogue. However, the evaluation in 2017 concluded that the focus must be directed towards enhancing the resilience of critical entities. In the conditions of evolving security challenges, risks and threats, Directive 2022/2057 was adopted in December 2022. The member states of the European Union are required to harmonise and adopt strategic priorities, management framework and necessary measures for the purpose of strengthening the resilience of critical entities, as well as a policy framework for coordination and information exchange. Additionally, mandatory measures for all designated critical entities include managing information security risk, exchanging information with competent authorities appointed in accordance with the NIS2 directive, and conducting security checks for individuals who come or may come into contact with information about the critical entity's operations.

III MANAGEMENT OF CRITICAL INFRASTRUCTURE IN THE NATIONAL SECURITY SYSTEM

1. National security system

The national security system is a subsystem of broader social systems, and primarily of the political system and legal order on whose principles it is based. The function of national security is realised through the actions of the entities within the national security system and includes the achievement, development and enhancement of national values and interests and the control of security challenges, risks and threats (Mijalković, 2018; Amidzić & Sikimić, 2024). In some countries, a special law is passed on the national security system, as is the case with the United States of America. On the other hand, we observe its key components in the examples of the Russian Federation, Austria, and Albania, while the definition of the national security system is not explicitly represented in the national security strategies. The third case is that countries define the national security system in their national security strategies, as seen in Slovenia and Serbia. In Bosnia and Herzegovina, the second approach mentioned above is represented, that is, the national security system is not defined by a special law or national security strategy, but it is possible to identify its key elements - armed forces, intelligence service and police.

The security system of a country consists of institutional, operational and normative components, and the sum of the activities of all elements of the system results in the system's operation. The institutional part consists of legislative, executive and judicial authorities, while the activities that establish and modify the security system represent the operational part of the national security system. The normative part comprises all norms that govern matters of importance for national security. Finaly, security entities are the state apparatus, non-state entities, government capacities and citizens, i.e. services, organisations, organs, bodies and institutions that, through their regular activities, directly or indirectly fulfill the function of security.

The management of the national security system falls under the jurisdiction of the highest bodies of the legislative and executive authorities, while the management of the system is performed by the subsystem components. The role of the judicial authority is conditionally executive, because the judicial authorities, although independent in performing tasks within their competence, act according to the laws enacted by the legislative authority (Forca, 2019). The type and strength of the legal act that regulates the area of critical infrastructure depends

on the political and legal system of the country, as well as the extent of changes needed to upgrad national legislation. When creating national public policies in the field of critical infrastructure security, which may be alternatives to existing policies or completely new, several stages and certain actors can be identified forming a policy network. The mutual interaction among all actors comes to the fore during the phases of initiating public policy, formulating public policy, implementing public policy, and evaluating public policy. In terms of actors, most authors distinguish between formal (state) and informal (non-state) actors, where formal actors are represented by the legislative and executive authorities (president, government, bureaucracy, agencies), as well as courts. For the purposes of this dissertation, we will focus on the parliament as a body of legislative power, while the roles of the president and the prime minister will be addressed within the role of the body of executive power. On the other hand, informal actors in public policy are individuals, political parties, interest groups, research organisations, media, etc.

The development of policy regarding the security of critical infrastructure is based on the Directive 2022/2557, as a source of the European Union law, and on national sources of law. Directive does not prescribe mandatory instruments for achieving results, but prescribes results that countries must achieve, provided that the legal norms of national legislation are not in conflict with the European source of law. Thus, Sweden and the United Kingdom are known as countries that have a developed framework for the protection of critical infrastructure, but do not have specific national laws regulating this area. On the other hand, countries such as Romania (Official Monitor no. 757 2010), Greece (Presidential Decree 39/2011), Hungary (Act CLXVI/2012; Sibalin et al 2020), and Croatia (Official Gazette of the Republic of Croatia 2013, 2022), have regulated the area of critical infrastructure with a specific national act. Finally, the nature and form of national sources of law directly depend on the political system, the organisation of the security system, i.e. the institutional, administrative, financial and personnel capacities of the countries (Sikimić, 2022c: 64).

2. The importance and role of the legislative authority as an actor of policy in the field of critical infrastructure security

State power is divided into several functions, most commonly legislative, executive and judicial, but there is an unbreakable link between these functions and it is essentially one power. Depending on whether a country has a presidential or a parliamentary system, the division of power is more or less rigid or flexible (Jović, 2019: 267). As a rule, the legislative power is

exercised by parliaments, as is the case in the leading European countries (Germany, France, Great Britain), Hungary and Bosnia and Herzegovina (Ćeranić, 2020).

The most significant tasks within the jurisdiction of the legislative authority as an actor of public policy in the field of critical infrastructure security include the following:

- ratification of international treaties and agreements in the field of critical infrastructure security,
- adoption of laws and other general acts such as strategies for the critical infrastructure security,
- approval of the budget required for the functioning of the security system and subsystems for the protection of critical infrastructure,
- management of other subsystems in the national security system.

In addition to the apparent legislative function of the parliament, the allocation of budget funds is also within the competence of the parliament. The main source for funding subsystems for the security of critical infrastructure is budget funds, and therefore the legislative authority holds a powerful tool in terms of monitoring government actions.

In addition to the legislative and budgetary functions, one of the functions of the parliament is its control function. The parliamentary model of control of the security system most often includes the adoption of laws defining the operation and organisation of the security system and subsystems, the control of the operation of the security system and subsystems, the approval of the annual budget for the security subsystems and the control of spending, the adoption of sector strategies on the operation of the security subsystem, the control of the legality of the security system's operation and protection of human rights (Ćeranić, 2023: 45).

As the practice in most countries of the European Union shows, parliamentary control can occur through a permanent parliamentary body that supervises and controls the operation of the security system and/or through special committees that can be formed in emergency situations, in case of political crises and the like (Ćeranić, 2023: 45). Thus, for example, the security and defense committee in many parliaments represents a political body responsible for the supervision of police and military structures, reviews and reports to the parliament on draft laws in the field of security and defense (Ćeranić, 2023: 47). In the context of critical infrastructure, it should be mentioned that these committees have the capability to initiate the adoption of new legislation in the field of security.

3. The importance and role of the executive authority as an actor of policy in the field of critical infrastructure security

The executive authority is realised through the work of the government and the president of the state, participates in the adoption of laws and by-laws, manages the security system and its elements. The government usually proposes laws and submits them to the parliament. On the other hand, by-laws and regulations of lower legal force than laws regulating the operation of security systems and subsystems are passed by the executive authority independently (Ćeranić, 2023: 48).

Specialised bodies are often formed within the executive branch to manage the security system (Ćeranić, 2023: 48). This could be the Ministry of Security or a similar department, whose existence and scope of work are determined and defined by law.

In the context of the implementation and development of the national framework for the security of critical infrastructure, the role of the executive authority is crucial and indispensable. The entire security system with its subsystems falls under the executive authority which determines and implements domestic and foreign policy in the area of critical infrastructure security. Specialised government bodies (departments) or ministries propose to the parliament a national strategy, law or other general act that should establish and/or regulate the security subsystem at the state level with the primary task of providing critical infrastructure. In the most common approach in European countries, the aforementioned departments are made up of ministries responsible for certain sectors of critical infrastructure, or the ministries of interior are responsible for activities on the development of a national strategy for the resilience of critical entities.

Adopting a methodology for risk assessment of critical infrastructure is under the direct responsibility of the executive authority. It is a sub-legal document for which the executive authority holds the mandate, and this kind of document usually does not require approval by the parliament. A specialised body of the executive authority is designated as a national point of contact for the exchange of information on critical infrastructure, which can be within the department for civil protection affairs, the body for cybersecurity or similar.

Finally, the mechanisms for risk assessment, determination of critical entities, determination and implementation of measures needed to strengthen the resilience of critical entities, coordination and exchange of information on critical infrastructure fall under the auspices and direct responsibility of the executive authority. The role of individual departments

within the executive authority in the protection of critical infrastructure will be further discussed in the following pages.

4. The role of the judical authority in the critical infrastructure security

The role of the judical authority in the context of the critical infrastructure security is legal protection, that is, the courts verify the legality of specific acts enacted by the security subsystems. We can also say that the role of the courts is exclusively of a supervisory nature, and control is performed by different courts, depending on the legal system of a country. In the case of the illegality of an act, the court imposes sanctions such as removing the consequences of the impugned act, ordering compensation for the resulting damage and the like (Ćeranić, 2023: 49). On that occasion, the court does not delve into the material side of the story, but only examines whether the prescribed legal procedure has been followed in the specific proceedings. For example, a competent government body designates a certain company as a critical entity and instructs the management of the company to take measures to strengthen resilience. If the management of that company disagrees with the decision of the competent authority, they can file a petition and seek legal protection before the competent court.

5. The importance and role of the police and security services in the security of critical infrastructure

The police, in today's sense of the word, as a public, specialised and professional service, is a relatively new, i.e. modern institution. Although the term police is primarily associated with uniformed members of the internal security forces, this term also includes public service, government bodies and civil administration. The role of the police as an organisation depends on the social and state structure, that is, the specifics of the legal regime condition the specifics of the police work and the legal position of the individuals who perform police work (Paterson, and Williams, 2019). The development of the police in a modern state is determined by a number of internal and external factors (Cherney, 2018), and some of those factors include: the system of executive authority, security policy, economic, social, political conditions in which the police perform their activities (Schreier, and Leimbach, 2022; Patterson, and Williams, 2019). In a modern conditions, the police represent a state administration body whose main activity is focused on the performance of the security of the state, citizens and their property. The concept of the police is also associated with the concept of internal affairs.

The role of the police in securing critical infrastructure is twofold. On the one hand, it is reflected in the prevention and suppression of attacks on critical infrastructure, and on the other hand, it appears as an actor and bearer of the implementation of public policies in the field of critical infrastructure security. In preventing and suppressing attacks on critical infrastructure, the role of the police is crucial and indispensable. One of the reasons for the above lies in the legality and legitimacy of police action in the application of coercive mechanisms provided by the state and the people. This characteristic of the police organisation is not characteristic of private security companies to such an extent, regardless of the level of their equipment, human resources and overall capacities. The state and citizens will primarily call the police for help, and the police is and will remain the first organisation in the service of the state and citizens.

Competent ministries generally prepare national security strategies at the state level, while individual police organisations undertake assessments down to the local level. Some of the data contained in the security assessment include data on the geographical location, the names of inhabited places, the number of inhabitants, the national composition of the population, the list of critical infrastructure facilities, the state of public order and peace, the state of crime, the state of traffic safety, an overview of facilities considered to be crime hotspots, as well as a list of companies with different production facilities. The above data is taken into consideration when assessing the risk to critical infrastructure. The police must constantly work to prevent the commission of criminal offences and all illegal activities aimed at endangering critical infrastructure. To achieve this goal, the police form special departments with the primary task of protecting critical infrastructure from certain types of attacks and forms of crime.[20]

Direct field work covered by a police organisational unit is often condicted as an officer and patrol activity. Officer activities are carried out in cities, larger settlements, industrial and traffic centers, tourist locations, etc. (Andresen, and Shen, 2019). The patrol area is primarily organised according to the number of critical infrastructure objects, so that the size of the patrol area allows the foot patrol to visit the critical infrastructure object several times during one shift (Bland et al, 2021; Rumi et al, 2020). Among the regular police services, it is important

[20] For example, the protection of critical maritime infrastructures has become a top political priority, since the September 2022 attacks on the Nord Stream pipelines in the Baltic Sea, and German police are patrolling the North Sea and the Baltic Sea with “all available forces” following the recent explosions (Bueger & Liebetrau, 2023).

to mention the security service which directly protects critical infrastructure facilities by undertaking a wide range of measures and activities. Operational-preventive measures aim to prevent the activities of individuals and/or groups that are aimed at endangering critical infrastructure. With the constant presence of members of the police in the form of guards, with the support of officer and patrol activities and the use of technical means, measures are taken to physically secure critical infrastructure facilities. The regular security service also continuously implements anti-sabotage, technical and fire prevention measures, chemical-biological measures, health protection measures and other necessary measures.

The police must have information on persons who are under enhanced surveillance, those who have previously committed criminal offenses and misdemeanors, as well as individuals who, by virtue of their profession, can observe and obtain information about threats to critical infrastructure or preparation of attacks on objects of special importance. This is especially important when it comes to members of terrorist organisations or organised crime groups. Furthermore, in order to provide comprehensive protection, it is necessary to share knowledge with other relevant bodies and organisations involved in the protection of critical infrastructure. Law enforcement have to share information with government agencies, the national security and intelligence communities, providers of network and other key infrastructure services, technology and security product vendors, security experts, incident response teams, education and research communities, international standard-setting bodies and media. Also, the Directive 2022/2557 provisions aimed at ensuring effective employee security management will normally involve the processing of personal data. This is justified by the need to carry out background checks on specific categories of personnel, and any such processing of personal data will always be subject to compliance with the General Data Protection Regulation (see more in Sikimić 2022a). According to Article 12 of the Directive 2022/2557, "background check shall: (a) establish the person's identity on the basis of documentary evidence; (b) cover any criminal records of at least the preceding five years, and for a maximum of ten years, on crimes relevant for recruitment on a specific position, in the Member State or Member States of nationality of the person and in any of the Member States or third countries of residence during that period of time; (c) cover previous employments, education and any gaps in education or employment in the person's resume during at least the preceding five years and for a maximum of ten years" (Directive 2022/2557: Article 12). The aforementioned data are in the possession of the security services, i.e. the police.

Unlike police duties, the execution of which requires the application of police powers and which are in the direct or indirect function of security, the goal of performing *other internal duties* is not the protection of security; they only serve the function of public security. By nature and character, other internal affairs are mainly administrative and professional (non-administrative) affairs of the administration. In terms of the way they are conducted, they are not characterised by the concreteness and immediacy of police action, which is why they can be carried out by another body in addition to the police (Milidragović et al, 2019). In the legal sense, the main task of the police is to enforce laws and/or to supervise the enforcement of laws within their jurisdiction. Other internal affairs that serve the function of security, in the context of protecting critical infrastructure, represent the police as a security structure that monitors events in the country and the region, and proposes the improvement of regulations in terms of organising preventive and repressive measures within its jurisdiction.

6. Inteligence and security of critical infrastructure

From national security and intelligence services, political authorities demand data and assessments that encompass all areas of social life, including the security of critical infrastructures. Terrorist acts aimed at critical infrastructure can symbolise an attack on the constitutional order, while cyber-attacks can paralyse numerous infrastructural systems (Lehto, 2022). The paralysis of critical infrastructure in the information and communication technology sector leads to disruptions in the functioning of almost all other critical sectors, supply chain crises (see more in Watney, 2022), market flow disruptions and social unrest. Therefore, intelligence agencies collect information on threats to critical infrastructure (Alqudhaibi et al., 2023) and, in order to protect the state's vital interests, intelligence activities are conducted against current and/or potential internal and external adversaries. The task of intelligence activity is to provide answers regarding the capabilities of adversaries, their intentions and the potential impacts on national security and the achievement of national objectives (Mijalković, Milošević & Ćeranić, 2023).

The highest level of organisation of intelligence activity is represented by intelligence services - specialised organisations of the state apparatus. In response to modern security threats to national security and critical infrastructure, such as new technologies and artificial intelligence, the intelligence community adapts and forms different types of intelligence organisations. One intelligence service of particular importance for the security of critical infrastructure is the electronic intelligence service, and the intelligence method most

organisations often employ is the *Technical Intelligence method* (TECHINT). Within this method there are subsystems such as *Signal Intelligence* - SIGINT,[21] *Imagery Intelligence* - IMINT[22] and *Information Technology Intelligence* - ITINT. ITINT implies the use of the most modern information technology for collecting intelligence data from open information systems - *Net open source intelligence*, and unauthorised access to unprotected computer networks - *Hackers intelligence* (HACKINT) (Mijalković, Milošević, & Ćeranić, 2023). In the future of critical infrastructure protection, it is expected that ITINT methods will prevail, as well as the development of information security capacities.

The products of intelligence activity can be different, depending on who they are intended for, the time frame, the territory, etc. Thus, tactical intelligence data is intended for immediate use and application in the field, and the process from information to intelligence data is short-lived (Jensen, McElreath, & Graves, 2018). This type of intelligence activity can be applied in case of a visit of a certain delegation or working group (e.g. potential investors) to a critical infrastructure facility. In that case, the security coordinator of the specific infrastructure needs to obtain data on the individuals arriving in a very short period of time and, based on that, determine the permitted or restricted visiting zones. On the other hand, strategic intelligence activities require much more time because they involve analyses of various long-term issues, economic implications and potential consequences for critical infrastructure and national security. The products of strategic intelligence activities undergo multiple verifications and are delivered to high-ranking leaders and national policy makers, and the intelligence activity process is conducted both domestically and internationally (Jensen, McElreath, & Graves, 2018). Quality intelligence activity should be constant, even if it does not always improve the security policy, but serves as a confirmation of the correctness of existing policies and activities (Leslau, 2010).

In accordance with the needs of national security and certain areas of interest, specialisation of tasks is conducted in modern intelligence and security systems and specialised departments are developed within existing and/or new intelligence organisations. Thus, the Republic of Croatia, through the Cyber Security Act, which incorporates the legal acquis of the European Union on cyber security (NIS2 Directive) into its legislation, has prescribed that the tasks of the central state body for cyber security will be performed by the Security and

[21] Collecting and processing intelligence data obtained through the interception of radio communications and other sources of electromagnetic radiation.
[22] This refers to intelligence imaging and includes general satellite surveillance and the use of infrared rays and other advanced technologies for photography.

Intelligence Agency (National Gazette of the Republic of Croatia, 14/2024). More precisely, the existing bodies of the intelligence agency of the Republic of Croatia will be transformed into the National Cyber Security Center (NCSC-HR) (Cybersecurity, 2024). Allegedly, the aforementioned body will be in charge of coordinating the implementation of security measures and providing assistance in resolving cyber attacks. During the public discussion of the proposal in the Croatian Parliament, examples of similar solutions in Denmark, Spain and Greece were cited, as well as examples from Germany and Italy, which initially established their cyber security centers within the security and intelligence system and later divided them into separate agencies (tportal, 2024). In the Western Balkan countries, there is one intelligence-security service that deals with both intelligence and counterintelligence activities, and it is realistic to expect transformations of individual organisational units within these services, in the direction of aligning with the needs of national policy in the context of European integration.

Finally, good and effective intelligence activity is essential for the security of critical infrastructure, and it begins when security policymakers clearly define the problems and needs in the field of critical infrastructure. However, good intelligence activity does not guarantee that the policies enacted will also be effective (Leslau, 2010). After receiving precise and accurate intelligence data, policy makers are left with the decision of whether and to what extent they will use the data obtained.

7. The importance and role of the military in the defense of critical infrastructure

The function of defense is realised individually, with one's own forces, or integratively, through collective defense and alliances (Jurišić, 2021). The armed forces implement measures to protect against enemy attacks, militarily defend the identity, state territory and people, with the purpose of the military being peace (Stanar, 2021). In addition to their basic purpose in the context of the defense power of the state, in democratic countries military structures are used for tasks that are not typically military (Amidzić & Sikimić, 2024). An organisation with trained personnel, a unique system of command and control, possession of equipment, land, air and maritime components is an irreplaceable element of the security system in the protection of critical infrastructure, both in war and in peace. Some of the tasks of the armed forces in the context of the protection of critical infrastructure are: intelligence and security tasks significant for the defense of the country, cyber and crypto-protection, development and the use of new military technologies, production and trade of military equipment and machinery (Besenyő &

Málnássy, 2022), joint civil-military operations in air traffic management, health, chemical, biological and radiological protection, assistance to civil authorities in conditions of natural disasters, etc (Nagy, 2023).

Military intelligence and security services collect data and information of military, military-political and military-economic nature, which are also significant for the protection of critical infrastructure (The Military Intelligence Agency of Republic of Serbia, 2024). Data and information on industrial security hold particular importance (Military Security Agency, 2024), as well as data on the production and proliferation of weapons and military equipment (Matz, 2022), which can be used in (terrorist) attacks on infrastructure facilities and structures.[23]

Within the armed forces, military police are also organised with tasks such as securing important military facilities and persons, and regulating military road traffic. In the event of threats to critical infrastructure on a larger scale, it is possible to organise joint military-police forces that will be engaged in restoring normal functioning of critical infrastructure.

In some countries, bodies responsible for cyber security are formed within the defense sector, such as the Military National Security Service's Cyberspace Operations Centre in Hungary (Brader, 2024). "National cyber security is based on military cyber security, and so there can be no national cyber security strategy without a military one" (Kovács, 2023).

The prominent function of critical infrastructure security is also collective defense (Biçakci, 2022; Böröcz, 2021; Georgescu & Tudor, 2015; Maigre, 2022). In 2023, NATO set strengthening national and collective cyber defense with an emphasis on critical infrastructure as a priority goal for its allies. In the protection of critical infrastructure, NATO has three basic tasks: deterrence and defense, prevention and crisis management, and cooperative security. The focus is on protecting one's own networks, operating in cyberspace and assisting allies in this area. At the Supreme Headquarters Allied Command Europe (Mons, Belgium), the NATO Cyber Security Centre (NCSC) is located with the role of centralised coordination in cyber defense. Information and best practices are exchanged with member countries of the alliance in order to develop national capacities for cyber defense. NATO Cyber Rapid Reaction Teams are also on constant alert, and in accordance with the needs and approval of the alliance, they engage in specific defense actions in some of the allied countries (Cyber defence, 2024).

[23] In scientific analyses of the arms trade, Ukraine is considered to have been the epicenter of the post-Soviet arms market. In the last decade of the 20th century, losses exceeding $32 billion were identified, which is the estimated value of illegally appropriated stockpiles of weapons and ammunition that were resold to terrorist and insurgent groups in Sierra Leone, Colombia and Liberia (United Nations Office on Drugs and Crime, 2024).

8. The importance and role of civil protection organisations in the protection of critical infrastructure

The function of protection and rescue has been known since the beginning of social communities, while civil protection as a state function developed in the period from the beginning of the First World War to the end of the Second World War. Depending on the specific political structure, some countries have an independent civil protection organization whitin the governments such as in Bosnia and Herzegovina (The Republican Administration of Civil Protection of Republika Srpska, 2024; The Federal Administration of Civil Protection, 2024). On the other hand, in a certain number of countries the mechanism of civil protection is within the ministries of defense like in Switzerland (Federal Office for Civil Protection FOCP, 2024) or within ministries of interior like a law enforcement body with national competence in Hungary (The National Directorate General for Disaster Management of the Ministry of Interior, 2024) and Serbia (see more in Djukić & Vuletić 2023). Civil protection activities are aimed at protecting and saving human lives, material and cultural assets from all kinds of natural disasters and disasters caused by human actions. This includes the consequences of terrorist activities, technological, radiological or ecological disasters, sea pollution, hydrological instability and emergency health situations. (Regulation (Eu) 2021/836, 2021: Article 1).

The significance and role of civil protection in strengthening resilience and protecting critical infrastructure are indispensable and manifest in a wide range of their activities, and we cite a few examples: providing information to the population about dangers and methods of prevention, conducting training for both population and members of civil protection, alerting the public to existing or potential accident through the alert centres, assisting and protecting the population through the implemention of evacuation measures, providing food, medical aid and sanitary assistance, undertaking recovery measures including the reconstruction of essential infrastructure to normalise living conditions, conducting decontamination and cleaning the affected areas.[24]

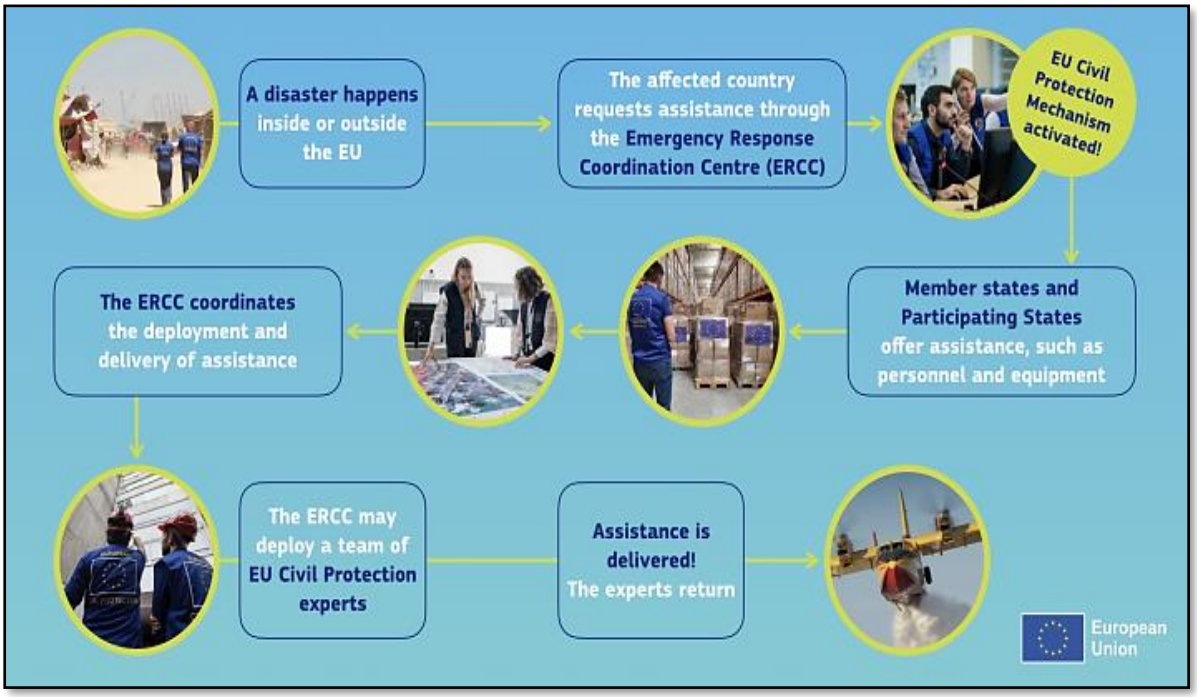
In this context, it is crucial to emphasise the importance of communication and coordination with other government departments, business entities and representatives of the local community. In the event of damage, destruction or contamination of water supply facilities, it is necessary to ensure the supply of clean water from other areas. Road clearing is

[24] Civil protection tasks can also include emergency burial, which the world had the opportunity to see after the devastating earthquakes in Turkey and Syria on February 6, 2023, when over 50,000 people died.

carried out in cooperation with business entities that have the necessary machinery, and this activity in most cases precedes the rescue from the ruins and ensures passage for rescue teams and first aid units. Finally, the services responsible for environmental protection should be included in the activities on the removal of ruins (Mlađan, 2015: 390-393). Citizens are also included as subjects within the protection system, and their rights and obligations in emergency situations are legally regulated. In the Republic of Serbia, the Republic of Croatia and Bosnia and Herzegovina, citizens are required to acquire skills for protection and rescue and to take measures for personal, mutual and collective protection. Citizens are obligated to accept assignments in civil protection units, participate in protection and rescue operations[25] and provide machinery, equipment and other material and technical resources necessary for carrying out essential work to protect human lives and critical infrastructure (Official Gazette of Republic of Serbia, No. 87/2018; National Gazette of the Republic of Croatia, No. 82/15, 118/18, 31/20, 20/21 and 114/22; Official Gazette of the Republic of Srpska, No. 121/12, 46/17 and 111/21).

The described role of civil protection mechanisms in the protection of critical infrastructure comes to the fore most in the circumstances of emergency situations. Especially in the case of natural sources of danger, disasters do not know national borders and the response must be common (Council Regulation (EU) 2016/369, 2016). In October 2001, the European Commission established the EU Civil Protection Mechanism whose members are all the countries of the European Union plus ten more countries, namely: Albania, Bosnia and Herzegovina, Iceland, Moldova, Montenegro, North Macedonia, Norway, Serbia, Turkey and Ukraine. The role of this body, more precisely its Emergency Response Coordination Center (ERCC), is to serve as a single point of contact and ensure a coordinated response of national bodies, the development of higher common standards and the exchange of best practices.

[25] Certain categories of citizens, such as pregnant women and mothers with children up to ten years of age, persons with disabilities and persons who care for them, are exempted from this obligation.



Picture 2: How the EU Civil Protection Mechanism works[26]

The Emergency Response Coordination Center operates 24/7 and is authorised to assist any country affected by a large-scale disaster at the request of national authorities or United Nations bodies. It is equipped with emergency communication and monitoring tools through the Common Emergency Communication and Information System (CECIS), an Internet application for warning and information that enables the exchange of information in real time[27] (European Commission, 2023).

In addition to the European mechanisms, there is also the International Civil Defense Organisation (ICDO) which was officially established in 1972 with headquarters in Geneva. This organisation brings together national structures of civil protection from all over the world with the aim of establishing cooperation and mutual solidarity. The main pillars of its activities are educational activities, Internationl Monitoring Coordination Center and Humanitarian assistance (ICDO, 2023).

[26] Image taken from the official website of the European Civil Protection and Humanitarian Aid Operations. Available at: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en?etrans=hr. Accessed: November 26, 2023.
[27] Active emergencies, ECHO DAILY Flash availabe at: https://erccportal.jrc.ec.europa.eu/#/echo-flash-items/latest. Accessed: May 06, 2024.

9. Supplementary security entities in the field of critical infrastructure

Local communities, public services, enterprises and citizens have certain resources that can be used to secure critical infrastructure.

In urban or municipal territories, a form of decision-making and management is organised directly by residents or through elected representatives. The professional services in charge of city security are an integral part of the municipal administration, and among their competences the most common are security policies on the territory of the local community and proposals for specific solutions for certain security problems. The city authorities develop protection and rescue plans, make decisions on implementing measures in response to emergency situations, whereas civil protection tasks and security authorities operations are organised in accordance with the characteristics of the local community. Managing critical infrastructure is an integral part of the responsibilities of local self-government, and strengthening the resilience of critical infrastructure is a prerequisite for the development of the local community and the improvement of the citizens' quality of life.

The construction and maintenance of critical infrastructure is the foundation of every functional living environment for people, and local communities are responsible for spatial planning, urban development, construction and maintenance of telecommunication and energy infrastructure, issuing permits for opening businesses and industrial facilities, promoting investments and supporting the development of local industry (Amidzić & Sikimić, 2024). At the level of the local community, a communal police are established whose responsibilities commonly include maintaining public order in certain sectors of critical infrastructure. In the first place, it concerns the sectors such as water supply, drainage of atmospheric and waste water, transportation and disposal of municipal and other waste. In addition, communal police most often oversee and control passenger transportation in urban and suburban traffic, fire protection, noise protection in the environment and provide assistance to city authorities (Mijalković, 2015: 304). Members of the communal police have powers which, depending on the country, differ to a greater or lesser extent from the powers of the public police. For example, the Municipal Police in Rome, Italy, known as Corpo di Polizia Locale di Roma Capitale, is responsible, among other things, for ensuring compliance with and enforcement of regulations related to public gatherings. During natural disasters, it carries out coordinated Civil Protection rescue services, even outside Rome (Get to know the Local Police Force of Rome Capital, 2024). Communal police in the capitals of the Netherlands, Germany, Spain and

other European countries have similar powers (see more: Guàrdia Urbana de Barcelona, 2024; Ordnungsamt, 2024).

Public services, enterprises and legal entities in certain areas also play a role in preserving national security and protecting critical infrastructure. In this context, public services in the field of health, education, social protection, legal entities in transportation, telecommunications, public information, electronic and print media, as well as companies engaged in the production of equipment and resources for security services, protection and rescue can be highlighted.

Finally, the resilience of critical infrastructure cannot reach its maximum level until citizens personally engage and incorporate the rules of conduct in protecting critical infrastructure into the general culture. Incorporating a security culture into the general culture is achieved through the cumulative acceptance of at least two complex actions. One is the communication of competent authorities with citizens, the exchange of knowledge and experience in various types of security (physical, property, health, economic security, etc.). The other part of the process is the influence of citizens on each other in developing awareness that individual reaction and behavior can create a threat, but also positive effects for personal and collective security. In case of necessity, citizens are mobilised during search and rescue in emergency situations, as well as during wartime, and the formation of attitudes about national values and interests is strongly influenced by the media.

10. The importance and role of non-state entities in the field of critical infrastructure

Strengthening the resilience of critical infrastructure is inevitably influenced by the relationship between government institutions and private agencies. In order to ensure the integrity of the framework for protecting critical infrastructure, it is necessary to include non-state security entities and cooperate and exchange information between the public and private security sectors (Besenyo & Feher, 2020). Among the non-state entities participating in the protection of critical infrastructure, private security and military agencies are generally distinguished, while public-private partnerships are recognised as social and technical means in building the resilience of critical infrastructure. Available publications mostly analyse this partnership in the context of cyber security, while a few deal with other sectors such as transportation, energy and health (Ampratwum, Osei-Kyei, & Tam, 2022).

Private military companies typically offer security and protection services for vital infrastructure facilities in zones of insurgency or military conflict, with their most frequent

clients being multinational companies in the mining industry. “For example, mining giant Freeport-McMoRan employed Triple Canopy to protect its vast mine in Papua, Indonesia, where there is an insurgency. The China National Petroleum Corporation contracts DeWe Security to safeguard its assets in the middle of South Sudan’s civil war” (McFate, 2019: 4-5).

The services of private security entities include measures such as physical security, video surveillance and access control, detection systems, fire protection systems and other technical measures, as well as personnel training (Amidzić & Sikimić, 2024: 43). The physical-technical protection system is a set of measures and actions of the security service and technical equipment of the mechanical and electronic protection system. The security service supervises critical infrastructure, where threat and risk analysis is the task of physical security, while various software solutions, modeling and simulations can be used to verify the effectiveness of physical security measures. An integrated protection system enables centralised control of all events in the system of one or more dislocated facilities from a central control station (Maksimović, 2022).

The development of the capabilities of the military and security agencies in all directions is supported and controlled by the state, but in the cyber operational space, the innovations and capabilities of the private sector are often ahead of the public and military sectors. Neither the national security nor the military agencies can keep up with the speed at which IT solutions are developed in large private companies, which is supported by the fact that the salaries for experts in the private sector significantly exceed the finances offered by the military or security services. By means of extensive sensor networks, private global companies have the ability to gather intelligence on cyber threats and appear as a more or less reliable source of information used to understand threats and conflicts in cyberspace.[28] On the other hand, one of the challenges in the event of a conflict is that private IT companies, which are critical infrastructure, generally protect themselves or hire other private agencies. Insufficient connection of private agencies with military or government services can result in ineffective protection of this critical infrastructure (Krasznay, 2024).

The integrity of managing critical infrastructure in the national security system is achieved through the joint action of formal and informal actors in public policy, the state apparatus, non-state entities and citizens. Passing strategies and laws in the field of critical

[28] Some military analysts claim that private domestic and global companies, as well as their volunteers and recruits, played a key role in Ukraine’s cyber defense, and that Ukraine witnessed the attack of artificial intelligence (see more in: Russel, 2023; Adam, 2024).

infrastructure falls under the jurisdiction of legislative authority, while the role of the executive authority is crucial and indispensable in implementing adopted regulations. Governments most often act as proponents of public policies and independently pass sub-legal guidelines in the field of critical infrastructure security, while legal protection falls under the jurisdiction of courts. The work of the police is aimed at preventing and suppressing attacks on critical infrastructure, while the work of intelligence services focuses on collecting data of importance for critical infrastructure in the function of national security. The armed forces implement measures to protect against hostile attacks, while civil protection organisations play a prominent role in protecting critical infrastructure in emergency situations. The completeness of managing critical infrastructure in the national security system is achieved through the engagement of the private security sector, local community, public services, companies, media and citizens.

IV POLICY, STATE AND PERSPECTIVES IN THE FIELD OF CRITICAL INFRASTRUCTURE SECURITY IN BOSNIA AND HERZEGOVINA

1. Constitutional and political organisation of Bosnia and Herzegovina

In order to examine the institutional and regulatory aspect of the current state and improve critical infrastructure security in Bosnia and Herzegovina, it is necessary to consider the characteristics of this country from the perspective of its constitutional and political structure, the jurisdiction of certain institutions in terms of the adoption and implementation of regulations, legislative procedures and public policy in the field of critical infrastructure security at all levels of government.

Bosnia and Herzegovina was constituted by the Dayton Peace Agreement as a democratic, multi-ethnic and internationally recognised state with two entities - Republika Srpska and the Federation of Bosnia and Herzegovina. The agreement consists of 11 annexes which establish the basic principles of the state legal order, civil and military issues. In addition to the centrally organised Republika Srpska and the Federation of Bosnia and Herzegovina, which consists of 10 cantons, the current administrative division also includes the Brčko District of Bosnia and Herzegovina. It is a separate territorial unit and common property of two entities (Mijalković, Milošević, & Ćeranić, 2023: 404).

The Constitution of Bosnia and Herzegovina is an integral part of the Dayton Peace Agreement, i.e. its Annex 4, which is not the usual way of adopting a constitution. It was created and proposed by the International Community, and was accepted by authorised representatives of the former Republic of Bosnia and Herzegovina, authorised representatives of Republika Srpska and authorised representatives of the Federation of Bosnia and Herzegovina.

Today, Bosnia and Herzegovina is a federal state and a form of state-legal organisation in which sovereign authority and jurisdiction are divided between a common sovereign state and lower, non-sovereign federal units. The constitutional order of Bosnia and Herzegovina is based on the principle of equality of three constituent nations and two entities (Kunić & Karan, 2012: 185-187). The entities prescribe in their laws the conditions for acquiring and terminating entity citizenship, and citizens of any entity are also citizens of Bosnia and Herzegovina. One of the fundamental principles of the constitutional organisation of Bosnia and Herzegovina is the presumption of jurisdiction in favor of the entities, which means that the Constitution

defines that all state functions and powers that are not explicitly given to the institutions of Bosnia and Herzegovina by the Constitution belong to the entities. According to Article III of the Constitution, responsibilities of the institutions of Bosnia and Herzegovina are:

- foreign policy,
- foreign trade policy,
- customs policy,
- monetary policy,
- finances of the institutions and for the international obligations of Bosnia and Herzegovina,
- immigration, refugee, and asylum policy and regulation,
- international and inter-entity criminal law enforcement, including relations with Interpol,
- establishment and operation of common and international communications facilities,
- regulation of inter-entity transportation,
- air traffic control (The Constitution of Bosnia and Herzegovina, 1995).

The Constitution of Bosnia and Herzegovina foresees the organisation of state authority according to the principle of division of powers. Legislative power is exercised by the Parliamentary Assembly of Bosnia and Herzegovina, while the bodies of executive power are the Presidency of Bosnia and Herzegovina and the Council of Ministers. The Constitutional Court of Bosnia and Herzegovina holds a constitutional and judicial function (Kunić & Karan, 2012: 221). Although not defined by the Constitution, Bosnia and Herzegovina also acquired judicial power through the transfer of jurisdiction.

According to the Constitution of Bosnia and Herzegovina, issues of security and defense are under the jurisdiction of the entities. In 2005, with the Law on Defense and Amendments to the Constitution of Republika Srpska, the unified Armed Forces of Bosnia and Herzegovina were formed and responsibilities from the field of defense were transferred to the institutions of Bosnia and Herzegovina. At the same time, entity laws on defense and the army were repealed, and the Army of Republika Srpska officially ceased to exist on January 1, 2006. The same happened with the Army of the Federation of Bosnia and Herzegovina, which until then consisted of two components - the Army of the Republic of Bosnia and Herzegovina and the Croatian Defense Council[29] (Ćeranić, 2020: 192).

[29] During the war in Bosnia and Herzegovina, the armed forces of the conflicting nations were formed: the Army of Republika Srpska (the army of the Serbian people), the Army of the Republic of Bosnia and Herzegovina (the

Today, the Ministry of Security of Bosnia and Herzegovina, the Ministry of the Interior of Republika Srpska, the Federal Ministry of Internal Affairs of Bosnia and Herzegovina, the Cantonal Ministries of Internal Affairs and the Brčko District Police are responsible for public security in Bosnia and Herzegovina. Since 2004, the country has also an Intelligence and Security Agency, which was formed by merging, that is, abolishing the entity services of state security.

Although the Dayton Peace Agreement prescribed a minimal administrative apparatus within the institutions of Bosnia and Herzegovina, with only three ministries serving as subsidiary bodies to the Presidency, today the country has an impressive number of ministries, agencies, institutes, directorates and various other bodies and organisations (Vranješ, 2020: 90). Opinions and views on their functionality, effectiveness and economic viability are divided with often contradictory attitudes from domestic and foreign authors, as well as holders of political positions.

1.1. System of government at the state level

Today, legislative power in Bosnia and Herzegovina is exercised by the Parliamentary Assembly of Bosnia and Herzegovina. The executive power belongs to the Council of Ministers and the Presidency of Bosnia and Herzegovina, while the judicial power is exercised by the Court of Bosnia and Herzegovina. The protection of constitutionality falls within the jurisdiction of the Constitutional Court of Bosnia and Herzegovina.

1.2. The system of government in Republika Srpska

Republika Srpska is a legal and social entity based on the principle of division of powers with emphasis on private property, a multi-party system and local self-government as the basis of the political system. It is the holder of sovereign power in the internal area, that is, 49% of the territory of Bosnia and Herzegovina, and it exercises its sovereignty through state bodies established by the constitution to perform republic functions. Constitutional and legislative power is exercised by the National Assembly and the House of Peoples, executive power is exercised by the Government as the operational body of the executive power and the President of the Republic as the head of state, while judicial power belongs to the courts. The House of Peoples, as a part of the National Assembly, has a legislative role in matters of vital national interest of any of the constituent nations.

army of the Muslim, later Bosniak people) and the Croatian Defense Council (the armed formation of the Croatian people).

1.3. System of government in the Federation of Bosnia and Herzegovina

The Federation of Bosnia and Herzegovina encompasses 51% of the territory of Bosnia and Herzegovina has its central bodies that make decisions binding for the entire territory of the Federation. A parliamentary system of government with a dual executive, consisting of the President of the Federation and the Government, has been accepted. Federal units (cantons or counties) represent administrative-territorial entities and there are a total of ten of them, and the presumption of jurisdiction is placed in favor of cantons (Vlaški & Davidović, 2023). These are: Bosnian-Podrinje Canton, Herzegovina-Neretva Canton, Sarajevo Canton, Canton 10, Posavina Canton, Central Bosnia Canton, Tuzla Canton, Una-Sana Canton, West Herzegovina Canton and Zenica-Doboj Canton. The cantons have their own constitutions, laws and other characteristics, and their jurisdiction includes public safety, education, culture and spatial planning. More precisely, all matters that are not under the exclusive jurisdiction of the Federation belong to the cantons. The cantons have a uniform organisation with a president, assembly, government, ministries and judicial bodies (Vlaški & Davidović, 2023).

1.4. Brčko District of Bosnia and Herzegovina

With the formation of the Brčko District of Bosnia and Herzegovina, the revision of the territorial and political organisation was carried out by the Arbitration Decision of March 5, 1999 (officially established on March 8, 2000). This part of the territory was exempted from the jurisdiction of the entities and placed under the independent administration of the district, and under the exclusive sovereignty of Bosnia and Herzegovina. It includes the territory of the Brčko municipality within the borders of 1991. The reasons for the formation of the Brčko District are primarily of a political nature, due to the absence of a compromise between the entities regarding the disputed part of the border line.[30] Today, this part of the territory of 492 km^2 is a local self-government unit, both a city and a district (Vranješ & Vlaški, 2023).

The highest legal act of the Brčko District is the Statute and is based on the division of powers. Legislative power is exercised by the Assembly, executive by the Government and judicial by the courts, and the District has also its own police. In order to ensure that the interests of the District are recognised and protected, the Office of the Brčko District Coordinator in the Council of Ministers of Bosnia and Herzegovina is responsible for

[30] The formation of the Brčko District disrupted the territorial integrity of Republika Srpska, and domestic authors emphasise the disruption of direct road communication between Banja Luka and Belgrade, the main cities of Republika Srpska and Serbia.

representing the Brčko District to the Council of Ministers, as well as for establishing cooperation and coordination between the Brčko District and the institutions of Bosnia and Herzegovina, international organisations and embassies (Office of the Coordinator of Brčko District of BiH in the Council of Ministers, 2024).

Branches of government/level of government	**Bosnia and Herzegovina**	**Republika Srpska**	**Federation of Bosnia and Herzegovina**	**Brčko District of Bosnia and Herzegovina**
Legislative power	Parliamentary Assembly of Bosnia and Herzegovina * Office of the High Representative	National Assembly of Republika Srpska	Parliament of the Federation of Bosnia and Herzegovina	Assembly of the Brčko District
Executive power	Council of Ministers of Bosnia and Herzegovina Presidency of Bosnia and Herzegovina	Government of Republika Srpska President of Republika Srpska	Government of the Federation of Bosnia and Herzegovina President of the Federation of Bosnia and Herzegovina	Government of the Brčko District Mayor of the Brčko District

Table 4.1: Power holders in Bosnia and Herzegovina [31]

After the elaboration of the government system in Bosnia and Herzegovina, and considering the aspect of the implementation of the critical infrastructure security framework, we conclude that the entity governments are the main creators of public policy and essentially have the same responsibilities. Since they propose almost all adopted laws, they also have a monopoly in the exercise of legislative functions. In addition, governments propose budgets, execute laws, harmonise and coordinate the work of ministries and other administrative bodies, and appoint and dismiss officials in administrative bodies. The difference is that the competences of the Government of the Federation of Bosnia and Herzegovina are more complex due to the intricate internal organisation of this entity and the existence of exclusive competences between the Government of the Federation of Bosnia and Herzegovina and the cantonal governments. A similar role is played by the mayor who presides over the Brčko

[31] Source: Author's creation.

District Government, an atypical unit of local self-government whose territory is jointly owned by two entities, and which has its own legal order in terms of organisation and functionality.

2. European path of Bosnia and Herzegovina

Constant and extensive international intervention in Bosnia and Herzegovina should be replaced by the acquisition of membership in the European Union. This attitude is often expressed in the colloquial slogan "from Dayton to Brussels", and for such a journey, among other things, adjustments to the domestic legal system are necessary. In 2000, the European Union initiated the Stabilisation and Association Process for Balkan countries, and in 2003, the accession perspective was opened for all the countries of the Western Balkans. Among these countries, North Macedonia first obtained the candidate status in 2005, followed by Montenegro in 2010, Serbia in 2012, Albania in 2014, while Bosnia and Herzegovina was granted candidate status only in December 2022. In the period from 2003 to 2022, numerous bilateral agreements were signed between the European Union and Bosnia and Herzegovina, with the aim of preparing the country for accession to the European Community. The Stabilisation and Association Agreement was launched in 2008 and ratified by the member states of the European Union in 2011. However, it entered into force only on June 1, 2015. In the meantime, several other agreements were signed, such as the Visa Facilitation and Readmission Agreement and the Interim Agreement on Trade and Trade-Related Matters. Deeper integration with the European Union was achieved through the framework of the Common Foreign and Security Policy, the Common Security and Defense Policy,[32] and through the Instrument for Pre-Accession Assistance - IPA[33] (Jens, Galić, & Sekulić, 2023) .

Bosnia and Herzegovina submitted its membership application to the European Union in 2016, on the basis of which the European Commission prepared and published in 2019 the Opinion on Bosnia and Herzegovina's EU membership application. This document outlined 14 priority issues and, according to the the European Commission's assessment, only one of these criteria was fulfilled by 2022. Despite this evaluation, Bosnia and Herzegovina was granted

[32] In Bosnia and Herzegovina, the EUFOR mission - Operation ALTHEA - is currently active, headed by the Hungarian Major General László Sticz (Commander of the European Union Force in BiH, 2024), and the presence of European forces in this country has been constant since 2003. In the period until 2012, the police mission EUPM was in effect - The European Union Police Mission in Bosnia and Herzegovina.

[33] It is estimated that from 1996 to 2021, the European Union transferred about 3.5 million euros to Bosnia and Herzegovina. Data show that imports from European Union countries constitute about 60%, while exports account for approximately 75%, which signifies that the European Union is the main trading partner of Bosnia and Herzegovina (Jens, Galić, & Sekulić, 2023).

candidate status in December 2022, even though the conditions were not met. It is believed that this decision was significantly influenced by the development of the geopolitical situation, the policy of the Russian Federation and the political allocation of the candidate status for EU membership to Ukraine, Moldova and Georgia.

According to the general criteria of the European Union, which must be met by all member states, Bosnia and Herzegovina should guarantee the effective implementation of the Union law on its territory and develop specific mechanisms and procedures in order to minimise the problem of complexity and fragmentation at different levels of authority. Despite leaving conditions for closing the Office of the High Representative in Bosnia and Herzegovina (OHR, 2024), the European Commission stated that the work of this Office is incompatible with the sovereignty of Bosnia and Herzegovina, and therefore with membership in the European Union (Jens, Galić, & Sekulić, 2023).

The body in charge of monitoring and fulfilling the conditions for accession at the state level is the Directorate for European Integration of Bosnia and Herzegovina. The Directorate is a permanent, independent and expert body of the Council of Ministers, and its competences relate to the coordination of processes and activities resulting from integration into the European Union. In close cooperation with ministries and administrative bodies, the Directorate coordinates work on harmonisation of domestic legislation with European Union regulations, communication and organisation of training on the integration process, and acts as the main operational partner of the European Commission in the integration process of Bosnia and Herzegovina (The Directorate for European Integration, 2024). In the context of critical infrastructure, a crucial responsibility of the Directorate is the national integration program, namely aligning legislation with the legal acquis of the European Union.[34] The decision on the alignment procedure stipulates that the proposer of the regulations should create alignment instruments, and one of the initial steps to initiate the legislative procedure is to create a table showing the compatibility of the provisions of the draft regulation with the sources of the European Union, controlled by the Directorate[35] (The Decision on the procedure for aligning legislation of BiH with the EU acquis).

Monitoring of the integration process by the legislative authority falls under the jurisdiction of the BiH – EU Stabilisation and Association Parliamentary Committee (The BiH

[34] One of the tasks of the Directorate for European Integration of Bosnia and Herzegovina is to control the quality of official translations of domestic legal regulations into English.
[35] Appendix 2 contains a template of the Table of Concordance and Statement of Compatibility.

– EU Stabilisation and Association Parliamentary Committee, 2024). This committee considers all aspects of the relationship between the European Union and Bosnia and Herzegovina, especially the implementation of the Stabilisation and Association Agreement. It consists of members appointed by the European Parliament and the Parliamentary Assembly of Bosnia and Herzegovina, and it is chaired alternately by the head of the delegation of the European Parliament and the head of the delegation of the Parliamentary Assembly of Bosnia and Herzegovina (Rules of Procedure governing the EU-BiH SAPC, 2024).

Level of authority/body	**Coordinating bodies within the executive power**	**Coordinating bodies within the legislative power**
State level	– Directorate for European Integration	– Parliamentary Committee for Stabilisation and Association between the Parliamentary Assembly of Bosnia and Herzegovina and the European Parliament
Republika Srpska	– Ministry for European Integration and International Cooperation – Unit for European Integration within the ministries	– Committee for European Integration and Regional Cooperation
Federation of Bosnia and Herzegovina	– Office for European Integration – Office for Legislation and Harmonisation with European Union Regulations	– Committee for European Integration (in both Houses of the Parliament) – Unit for European Integration
Brčko District of Bosnia and Herzegovina	– Department for European Integration and International Cooperation	– Committee for European Integration

Table 4.2: Coordinating bodies for the European integration of Bosnia and Herzegovina [36]

In accordance with the constitutional arrangement and organisation of authorities in Bosnia and Herzegovina, a significant part of the work and fulfillment of obligations in the process of European integration falls under the responsibility of the entities. Thus, the Government of Republika Srpska states that "the prerequisites for the effective performance of related tasks in the field of European integration at the entity level include: an effective system and mechanism of coordination between the different levels of authority within Bosnia and

[36] Source: Author's creation.

Herzegovina, respecting their constitutional competences, institutional and personnel capacity, cooperation and joint engagement of entity institutions, as well as with institutions at the local level, and an effective coordination system within the Government of Republika Srpska" (EU integrations, 2024). By actively participating in this process, Republika Srpska demonstrates its commitment to join the European Union, continuously adjusting its legislation. One of the first steps taken by the Government of Republika Srpska since 2006 is the establishment of units for European integration within the ministries. These units are composed of a maximum of 3 executives, whose primary task is to act as contact persons and coordinators of activities within their ministries, to participate in the preparation and monitoring of the implementation of plans, and to organise activities related to the harmonisation of domestic legislation with European Union regulations and participation in European Union funds. The Ministry for European Integration and International Cooperation has been established, serving as the Republic's coordinator with the main task of fulfilling and monitoring the fulfillment of obligations from the Stabilisation and Association Agreement, participating in the drafting of normative acts for their harmonisation with the regulations of the European Union, cooperating with the institutions of the European Union in Bosnia and Herzegovina, and reporting to the Government on the accession process. "Planning a more efficient adoption of European Union law into the legal system of Republika Srpska in the coming period and building effective administrative and judicial capacities for its consistent application contribute to strengthening the institutions' ability to assume the complex obligations that future membership in the European Union will bring." Legal alignment with the European Union legislation is planned in accordance with the specific development needs of Republika Srpska and the realistic possibilities of implementing new solutions, while strengthening institutional and human capacities along with continuous training will contribute to a more effective fulfillment of the requirements of the integration process. Additionally, Republika Srpska will continue its institutional and coordinated active participation in the work of all joint working bodies formed between the European Union and institutions in Bosnia and Herzegovina" (EU integrations, 2024). The Committee for European Integration and Regional Cooperation has been established in the National Assembly of Republika Srpska, a body that discusses issues related to monitoring and harmonising the legal system of Republika Srpska with the legal system of the European Union (The National Assembly of Republika Srpska, 2024).

In order to fulfill entity obligations and join the European Union, two offices have been established within the Government of the Federation of Bosnia and Herzegovina, namely the Office for European Integration and the Office for Legislation and Harmonisation with

European Union Regulations. Among the tasks and responsibilities of the Office for European Integration are “developing methodology and guidelines, as well as the overall coordination of work in the process of European integration under the jurisdiction of the Government of the Federation, federal ministries and other bodies of the federal administration.” It also provides expert assistance and coordinates activities in the development of strategic documents, information and expert analyses, coordinates the European Union assistance program through participation in planning, allocation and monitoring of the implementation of the program, as well as the coordination of activities, supervision and reporting on the implementation of the Stabilisation and Association Agreement (FBiH Government Office for European Integration, 2024). The Government Office of the Federation of Bosnia and Herzegovina for Legislation and Harmonisation with European Union Regulations provides “expert legal opinions on preliminary drafts, drafts and proposals of laws, their compliance with the Constitution and legal system, and other regulations adopted by the Parliament of the Federation of Bosnia and Herzegovina, the President and Vice Presidents of the Federation of Bosnia and Herzegovina, the Government of the Federation of Bosnia and Herzegovina, i.e. the heads of federal administrative bodies and federal institutions. It ensures methodological unity in drafting federal laws, other regulations and general acts, provides expert assistance to federal administrative bodies and federal institutions in drafting laws and other regulations, examines and discusses issues of developing the legal system, determines refined texts of regulations adopted by the Government of the Federation of Bosnia and Herzegovina.” In order to provide expert assistance to federal administrative bodies and federal administrative organisations in drafting laws and other regulations, it organises expert seminars and training, and provides the Government of the Federation of Bosnia and Herzegovina with expert legal opinions on these regulations from the perspective of their compliance with the legislation of the European Union and European principles and standards, together with the Comparative Overview of the compliance of the provisions of the draft and draft laws and general acts with the EU legislation (FBiH Government Office for Legislation and Alignment with the EU acquis, 2024). In the Federation of Bosnia and Herzegovina, the aforementioned activities are subject to the control of the legislative power, which is carried out by the competent Committe for European Integration. This Committee is the working body of the House of Representatives of the Parliament of the Federation of Bosnia and Herzegovina (Parliament of the Federation of Bosnia and Herzegovina - Committees, 2024), while the House of Peoples has a Committee and a Unit for European Integration (House of the people - working bodies, 2024).

The involvement and coordination of public administration bodies and institutions of the Brčko District in the process of joining the European Union is the responsibility of the Department for European Integration and International Cooperation, which is part of the Government of the Brčko District (Department for European Integration and International Cooperation, 2024). The competences of the Department are essentially identical or similar to the competences of entities' bodies for European integration, and all activities are monitored by the Committee for European Integration within the Assembly of Brčko District.

According to the European Commission's report from November 2023, Bosnia and Herzegovina has 14 listed priorities[37] it needs to fulfill in order to become a member of the European Union (Bosnia and Herzegovina 2023 Report, 2023). Although the issue of critical infrastructure is not explicitly mentioned in the package of fourteen priority issues for the accession of Bosnia and Herzegovina to the European Union, work has been started in this area to align with the regulations and standards of the Union.

2.1. Policy in the field of critical infrastructure security

A country with a complex constitutional structure like Bosnia and Herzegovina benefits from the existence of uniform European Union guidelines in the specific area, especially in the context of harmonising regulations at the entity and state level. At the beginning of 2023, the EU Directive 2022/2557 on the resilience of critical entities entered into force, alongside with previously initiated intensified efforts towards Bosnia and Herzegovina's European integration process. In accordance with the current circumstances, on June 6, 2023, the Parliamentary Assembly of Bosnia and Herzegovina adopted a conclusion instructing the Ministry of Security of Bosnia and Herzegovina to draft a proposal for a law on critical infrastructure. The conclusion defined a deadline of 60 days, but even by the beginning of 2024, the requested proposal regarding critical infrastructure was not prepared.

Following the recommendations of Directive 2022/2557 and taking into account the specificities of the country, there is an attitude and intention to draft a law on critical infrastructure for the institutions of Bosnia and Herzegovina, while and at the same time the entities and Brčko District have to enact laws on critical infrastructure at their level of

[37] Appendix 3: Bosnia and Herzegovina 2023 Report, Key priorities.

authority.[38] It is of critical importance that the methodologies for identifying and determining critical infrastructure are harmonised or unified across all levels of authority.

The Ministry of Security of Bosnia and Herzegovina is responsible for these activities at the state level. This Ministry has no operational competence in terms of police affairs, while the police agencies within have their operational autonomy. Thus, in the context of critical infrastructure security, the Ministry of Security would have a normative role of an executive authority at the state level, but also a coordinating role in the exchange of information on critical infrastructure. There is a possibility and a proposal from experts to establish a multi-institutional coordination body within the Ministry of Security for the exchange of information on critical infrastructure. This body would include representatives of the institutions of Bosnia and Herzegovina, both entities and Brčko District. Decisions would be made by consensus and all parties would have to give their consent for certain information to be forwarded to another country/countries. This intention is based on reasons of a practical nature, i.e. cascading action of critical infrastructure. Due to the size of the territory of Bosnia and Herzegovina, it is almost impossible to imagine an example of a single critical infrastructure, the interruption of which would not have an impact in another entity or Brčko District, as well as in neighboring countries. For the same reason, the interviewed experts emphasise the need to define the inter-entity critical infrastructure in Bosnia and Herzegovina, modeled on the idea of European critical infrastructure.

In the context of the implementation of programmes and measures in the field of critical infrastructure security of Republika Srpska, the Ministry of Interior of Republika Srpska is responsible for the activities. In addition to this Ministry, the Ministry for European Integration and International Cooperation also plays an important role, as it is responsible for assessing the compliance of national legal frameworks with primary and secondary sources of European Union law (Amidzić & Sikimić, 2024), as well as the Agency for Information and Communication Technologies as the entity responsible for activities in the field of cyber security of Republika Srpska. Specific activities regarding the normative regulation of critical infrastructure in Republika Srpska started in 2016. The Ministry of Interior provided the Government of Republika Srpska with information that, due to the complexity of protecting

[38] Respondent 2: "One of the current extremely sensitive socio-political issues in Bosnia and Herzegovina is the issue of entity property. The initiation of an initiative to enact a law on critical infrastructure that would apply to the entire territory of the country, and also treat entity institutions, would very likely provoke certain divisions and activate various "political barriers" in the process of regulating this area. Such a situation would not bring anything good."

critical infrastructure and harmonising legislation with the acquis of the European Union, it is necessary to create an appropriate legal framework for the area of critical infrastructure, and in the same year a working group was appointed to draft the law. The National Assembly of Republika Srpska adopted the Law on Critical Infrastructures Security in the Republic of Srpska in July 2019, and the supervision of the implementation of this law is the responsibility of the Ministry of Interior of Republika Srpska (Amidzić & Sikimić, 2024). According to the assessment of the Ministry for European Integration and International Cooperation of Republika Srpska, the law is partially aligned with Directive 2008/114/EU, which was repealed by the adoption of Directive 2022/2557 on the resilience of critical entities. Two years after the adoption of the law, in 2021, the Methodology for Critical Infrastructure Identification and Risk Assessment for Critical Infrastructures was adopted. The Ministry of Interior claims that the Methodology adopted solutions from Directive 2022/2557 on the resilience of critical entities, although the Methodology was adopted almost two years before this Directive came into force. The Methodology for the Identification of Critical Infrastructures and Risk Analysis for Critical Infrastructures of Republika Srpska is classified as confidential and is not publicly available.

In 2023 an Interdepartmental Working Group was formed for the implementation of the Law on Critical Infrastructure Security of in the Republic of Srpska. The members of this body are representatives of the General Secretariat of the Government of Republika Srpska, all ministries in the Government of Republika Srpska and Civil Protection Administration, while there are no representatives of the private sector. The task of the Interdepartmental Working Group is to propose sector-specific measures to the competent public administration authorities, to identify critical infrastructure facilities and propose their designation, and to draft a by-law establishing the procedure for verifying entities and facilities of critical infrastructure. At the end of December 2023 the Ministry of Interior requested from the Interdepartmental Working Group that its members propose sector-specific measures for their sectors as soon as possible.

Activities to regulate the area of critical infrastructure have also been initiated in the Federation of Bosnia and Herzegovina. In September 2022 the Government adopted a conclusion ordering normative actions aimed at protecting critical infrastructure. On November 3, 2022, the President of the Government of this entity issued a decision on the appointment of a working group for the preparation of a preliminary draft of the law on the protection of critical infrastructure in the Federation of Bosnia and Herzegovina. The working group consists of 11

members, mostly representatives of ministries in the government of the entity and a representative of civil protection (Government of Federation of BiH, 2024). The activity holder is the Federal Ministry of Internal Affairs, which submitted the draft law on the protection of critical infrastructure in the Federation of Bosnia and Herzegovina to the legislative procedure. During 2023 the proposal of this act was on the agenda in the Parliament of the Federation of Bosnia and Herzegovina, but it has not been adopted yet (Laws, draft, 2024). The proposed document followed the solutions represented in Directive 2008/114/EU which is no longer in force. The Brčko District of Bosnia and Herzegovina also still does not have a legal framework that regulates the security of the critical infrastructure of Brčko District. Respondents in interviews claim that the Federation of Bosnia and Herzegovina and Brčko District are waiting for the law to be adopted at the state level, the provisions of which will be implemented in the entity and Brčko District law.

3. Positive legal framework for the security of critical infrastructure in Bosnia and Herzegovina

The only currently valid legal act that directly regulate the field of critical infrastructure in Bosnia and Herzegovina, i.e. part of its territory, are the Law on Critical Infrastructure Security in the Republic of Srpska (Official Gazette of the Republic of Srpska, No 58/19) and the Methodology for Critical Infrastructure Identification and Risk Assessment for Critical Infrastructures of Republika Srpska. According to the aforementioned law, "critical infrastructure refers to systems, networks and facilities of particular importance, the endangering or destruction of which would cause a serious disruption on free movement of people, transport of goods and the providing services, have negative impact of on internal security, well-being and lives of people, property, environment, external security, economic stability, and continuous functioning of public bodies" (Law on Critical Infrastructure Security in the Republic of Srpska, Article 2). Article 3 lists the sectors which critical infrastructure is determined from, namely:

- industry, energetics and mining,
- information-communication infrastructure,
- traffic,
- health care,
- utility services,
- water management,

- food and drinks,
- finance,
- production, storage and transportation of hazardous materials,
- public services,
- upbringing and education, and
- cultural and natural assets.

The Minister of Interior adopts the Methodology, as well as the decision on the determination of critical infrastructure, while sectoral measures are adopted by the competent authority from the sector which the specific critical infrastructure belongs to. In this part, the legislator has left the possibility for public bodies to consult professional associations (Sikimić, 2021). The law defines the protection of critical infrastructure as all activities aimed at ensuring the functionality, continuous operation and delivery of goods and services of critical infrastructure, as well as preventing threats to critical infrastructure. In each sector of critical infrastructure, it is necessary to appoint a security coordinator and a deputy (Sikimić, 2022c). These individuals may also be chosen from among the employees of the public administration body responsible for the specific sector. The person who is directly responsible for managing and protecting critical infrastructure can also be among the employees, and all responsible entities of critical infrastructure have the obligation to designate these individuals. There is an obligation to prepare risk assessment analyses which assess direct and indirect damage according to the identified possibilities of interruptions in work, as well as plans to ensure the operation of critical infrastructure. These documents can be an integral part of security plans that must be drawn up within one year from the date of receiving the decision on determining critical infrastructure and include measures to protect and ensure the continuation of the operation of critical infrastructure and the delivery of goods and services (Amidzić & Sikimić, 2024).

As direct damage, risk assessment analysis assesses the number of fatalities and/or injured individuals due to the interruption of the operation of certain critical infrastructure, economic losses or decrease in the quality of products and services, possible impact on the environment, impact on public trust, and loss of basic and public services. Furthermore, the long-term impact on the integrity of individuals and the community, the realisation of human rights and freedoms, long-term economic damage and the impact on the quality of the environment are assessed as indirect damage (Sikimić, 2022b).

The Ministry of Interior of Republika Srpska has been designated as the contact point for cooperation and exchange of information with related bodies of other countries, and the law also defines international critical infrastructure as infrastructure that is defined as critical between two neighboring countries (Law on Critical Infrastructure Security in the Republic of Srpska, Article 4, paragraph 8).

The analysis of the law shows that solutions are mostly taken from Directive 2008/114/EC, however, sectors determining critical infrastructure are more broadly set compared to the aforementioned Directive. The consequences of critical infrastructure interruptions are primarily focused on the number of killed or injured persons, while currently valid Directive 2022/2557 primarily refers to estimates of the number of users who rely on key services provided by the infrastructure. There is an intention to draft amendments to the existing law in Republika Srpska in the coming period, with the aim of more comprehensive alignment with the legislation of the European Union and the expected laws in the Federation of Bosnia and Herzegovina, Brčko District and at the level of the institutions of Bosnia and Herzegovina. Due to the confidentiality of the Methodology for Critical Infrastructure Identification and Risk Assessment for Critical Infrastructures, it is not possible to present an analysis of its provisions. Opinions are divided among respondents who had or have access to and were directly involved in the drafting of this act. Some respondents claim that the solutions are in line with Directive 2022/2557, while others state that the presented framework for determining critical infrastructure is based on the level of damage and the probability of occurrence of an emergency situation measured based on previous events. The same respondents believe that this is not a good solution and that risk assessments and analyses should not be solely the task of civil protection, and that other types of risk assessment, such as risk assessments of company operations, must also be included.

The Law on Critical Infrastructure Security in the Republic of Srpska defines the deadlines for the implementation of prescribed measures and activities. Within 18 months from the entry into force of this Law, the heads of the public administrative bodies were required to adopt sectoral measures and within six months from the date of adoption of the Methodology for Critical Infrastructure Identification and Risk Assessment for Critical Infrastructures to propose critical infrastructures from the sectors under their competencies and their level of criticality. Although the Law was adopted in 2019 and the Methodology in 2021, research results show that there are still no formally identified or named critical infrastructure/critical

entities, security coordinators or verified security plans in Republika Srpska (nor in Bosnia and Herzegovina as a whole).

In addition, an integral part of the contemporary European security framework for critical infrastructure are information security and personal data protection (Sikimić, Čihorić, 2022). The Law on Protection of Personal Data in Bosnia and Herzegovina is not aligned with the General Data Protection Regulation (GDPR), and the state and entity laws on information security are not aligned with the NIS2 directive.

4. Security system, state mechanisms and entities of critical infrastructure security in Bosnia and Herzegovina

"Bosnia and Herzegovina has its own security system and it functions despite the weaknesses that come to the fore in crisis situations" (Respondent 4). The elements of the security system of Bosnia and Herzegovina, i.e. its conventional entities at the state level, are: the Ministry of Security of Bosnia and Herzegovina, the Intelligence-Security Agency of Bosnia and Herzegovina and the Armed Forces of Bosnia and Herzegovina. At the entity level, these are the Ministry of Interior of Republika Srpska and the Federal Ministry of Internal Affairs along with ten cantonal ministries of internal affairs. In Brčko District, the security system is represented by the Brčko District Police (Ćeranić, 2023: 102). The listed ministries, as representatives of the executive power, are initiatiators and proposers of laws on the security of critical infrastructure in Bosnia and Herzegovina.

4.1. Ministry of Security of Bosnia and Herzegovina

The Ministry of Security of Bosnia and Herzegovina collects data of importance for the security of Bosnia and Herzegovina, engages in the prevention and suppression of crimes with an international and inter-entity element, primarily terrorism, drug trafficking, counterfeiting of domestic and foreign currency and human trafficking. It also develops and implements policies on immigration and asylum, protection of persons and objects, forensic examinations and expert reports, provides support to police bodies and conducts training and professional development of personnel in accordance with the needs of the police bodies of Bosnia and Herzegovina (Official Gazette of BiH, 5/03, 42 /03, 26/04, 42/04, 45/06, 88/07, 35/09 and 103/09: Article 14). The Ministry does not have operational responsibilities in terms of police affairs, but it includes the following administrative organisations with operational independence: Directorate for Coordination of Police Bodies of Bosnia and Herzegovina, Border Police of Bosnia and Herzegovina, State Investigation and Protection Agency (SIPA),

Agency for Forensic Investigations and Expertise, Agency for Education and Professional Training, Police Support Agency and the Service for Foreigners' Affairs. It is also responsible for the coordination and harmonisation of entity ministries of internal affairs and Brčko District in the implementation of security tasks in the interest of Bosnia and Herzegovina. It implements international obligations and cooperation in the field of civil protection, coordinates the actions of entity civil protection services and harmonises their plans in the event of a natural disaster or other emergencies, as well as international cooperation with Interpol, Europol and other regional and international police organisations (Official Gazette of BiH, 5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09 i 103/09).

As one of the ministries in the Council of Ministers of Bosnia and Herzegovina, the Ministry of Security was tasked by the House of Representatives of the Parliamentary Assembly of Bosnia and Herzegovina to draft a bill on critical infrastructure and to take measures to establish a Computer Emergency Response Team (CERT) at the level of institutions of Bosnia and Herzegovina. It is also the bearer of activities at the state level and the coordinator of the regulation of critical infrastructure in Bosnia and Herzegovina.

The Ministry of Security is organised into sectors, namely: Sector for Protection and Rescue, Sector for Legal Affairs, Human Resources, General Affairs, Material and Financial Affairs, Sector for International Cooperation and European Integrations, Sector for Immigration, Sector for Asylum, Sector for Combating Terrorism, Organised Crime, Corruption, War Crimes and Misuse of Narcotics, Sector for IT and Telecommunication Systems, Sector for Protection of Classified Information, Sector for General and Border Protection and Inspectorate. In the context of regulating the area of critical infrastructure in Bosnia and Herzegovina, we emphasise the Sector for International Cooperation and European Integrations, which is further divided into the Department of International Cooperation, the Department of European Integration and the Department of Combating Trafficking in Human Beings. This Sector manages the procedures for concluding international agreements, prepares proposals for the ratification of United Nations conventions, European and regional conventions in the field of security, ensures the adoption of international and European police standards, defines security priorities and policies, and participates in the preparation of laws, other regulations and by-laws in the field of security (Sector for International Cooperation, 2024). Of particular importance for the area of critical infrastructure is that the Sector for International Cooperation and European Integrations monitors and coordinates activities on the

implementation of agreements with the European Union, harmonisation of legislation and fulfillment of obligations related to European integration.

According to some respondents, the Sector for Protection and Rescue, which is divided into the Department of International Cooperation and Coordination, the Department of Strategic Planning, Protection and Rescue Measures, the Department of Structure and Training, and the Operational Communication Center 112, can serve as an example for the organisation of the coordinating body or the appropriate joint contact point for information on critical infrastructure in Bosnia and Herzegovina. Also, since 2023 the cooperation with EUROPOL (European Union Agency for Law Enforcement Cooperation) has taken place through the National/Joint Contact Point for Bosnia and Herzegovina within the Ministry of Security. All police agencies from the entity level, Brčko District and the state level of government are represented in this body consisting of 16 police officers, and other respondents believe that such a model could be established in the case of the exchange of information on critical infrastructure.

In the context of the critical infrastructure protection, the Directorate for the Coordination of Police Bodies of Bosnia and Herzegovina organises, coordinates and implements operational, physical and technical security measures for VIPs and facilities of state importance or interest, and assesses possible threats to protected persons and facilities. These typically include facilities of the institutions of Bosnia and Herzegovina (the building of the Presidency, the Council of Ministers of Bosnia and Herzegovina, the Parliamentary Assembly of Bosnia and Herzegovina, etc.), diplomatic and consular missions and residences of other countries in Bosnia and Herzegovina. In terms of protection of individuals under the Directorate's jurisdiction, security and escort services are provided to holders of the highest political positions in the institutions of Bosnia and Herzegovina, as well as to VIP delegations.

Security screening of individuals who come into contact with critical infrastructure data is one of the determinants of the resilience of critical entities in the context of Directive 2022/2557. Depending on the level of confidentiality, the State Investigation and Protection Agency and/or the Intelligence-Security Agency of Bosnia and Herzegovina conduct security checks for individuals, while the Ministry of Security issues permits for access to classified information.

4.2. Ministry of Interior of Republika Srpska

The Ministry of Interior of Republika Srpska performs state administration tasks related to protection against threats to the constitutionally established order and the security of Republika Srpska, as well as the protection of life and personal safety of citizens. The structure of the police in Republika Srpska is constituted according to the territorial structure of authority. Police duties include operational and professional tasks that ensure the protection of life, personal safety, human rights and freedoms, the protection of the constitutional order from violent threats and changes, and the security of Republika Srpska. Police duties also encompass the protection of all forms of property, the prevention of criminal acts, the detection of criminal acts, the maintenance of public order and peace, as well as the protection of certain individuals and facilities, the security of public gatherings, i.e., all permitted forms of mass gatherings of citizens (Official Gazette of Republika Srpska, No 57/16, 110/16, 58/19, 82/19, 18/22 и 55/23). The main organisational units at the headquarters of the Ministry include: Cabinet, Service, Police Committee, Police Director, Administration, Special Anti-Terrorist Unit, and Training Center, while outside the headquarters of the Ministry there are police administrations (Amidzić & Sikimić, 2024).

In the field of critical infrastructure, the Ministry of Interior is the proposer of the law, responsible by law for supervising the implementation of the law, and the contact point for exchanging information on critical infrastructure with other stakeholders. Several units and departments, including the Citizens' Petition Bureau, are organised within the Minister's Services. One notable unit is the Unit for International Cooperation and European Integrations, responsible for coordinating, consultating and aligning acts in the field of security and competence of the Ministry of Interior of Republika Srpska with the legal acquis of the European Union. This Unit presides over the work of the Interdepartmental Working Group for the Implementation of the Law on Critical Infrastructure Security in the Republic of Srpska.

Within their police jurisdiction, members of the Ministry perform officer and patrol activities, prevention and suppression of all forms of crime, including the fight against terrorism. As part of their regular activities, the members of the Administration for Protecting Persons and Buildings provide physical and technical security of persons and buildings that require special protection, undertake measures of anti-terrorist security, operational-preventive, preventive-technical, biological, chemical, sanitary and health security of persons they protect and directly participate in their implementation and application of appropriate technical means of protection at critical infrastructure sites. The Crime Police Administration

and the Administration for Police Support are responsible for implementing data protection measures and undertaking activities to prevent and suppress planned or committed criminal acts in the field of information security (Amidzić & Sikimić, 2024).

4.3. Federal Ministry of Internal Affairs and Cantonal Ministries of Internal Affairs of Bosnia and Herzegovina

In the Federation of Bosnia and Herzegovina police is organised in accordance with the power structure. The entity government includes the Federal Ministry of Internal Affairs, while each canton has its own Ministry of Internal Affairs. Within the Federal Ministry, there is the Police Academy, Inspectorate, Internal Audit Unit and Federal Police Administration, as well as Sector for Legal Affairs, Sector for Material and Financial Affairs and Sector for General and Joint Affairs. Internal affairs under the competence of the Federal Ministry are as follows: prevention and detection of criminal acts of terrorism, inter-cantonal crime, trafficking of narcotics and organised crime, as well as finding and apprehending the perpetrators of these criminal acts and bringing them to the competent authorities; security of certain persons and buildings of the Federation; education, professional training and improvement, acquisition and termination of citizenship. Operational tasks under the jurisdiction of the Federal Ministry of Internal Affairs are performed by the Federal Police Administration (Official Gazette of FBiH, 81/14). The Government of the Federation determines by regulation which persons and buildings of the Federation require special security measures and regulates the method of their security, which is operationally carried out by the Federal Police Administration.

In addition to its primary police role, the Federal Ministry of Internal Affairs is in charge of implementing the security framework for the protection of critical infrastructures in the entity. It acts as the proposer of the preliminary draft of the Law on the Protection of Critical Infrastructure in the Federation of Bosnia and Herzegovina, and the document was submitted to the legislative procedure in July 2023.

The Federation of Bosnia and Herzegovina has a decentralised police system with elements of coordination. Cantonal Ministries of Internal Affairs act completely independently in the implementation of their tasks and tasks. They are not hierarchically subordinate to the Federal Ministry of Internal Affairs and are not an integral part of its organisational structure. These ministries are subordinate to the cantonal authorities and financed from their budgets (Miličević, 2023). The organisation of the police in the cantons is established according to the shared competences between the Federal and Cantonal Ministries of Internal Affairs. The

cantons are responsible for establishing and supervising police forces with a uniform federal uniform and cantonal insignia. Each cantonal assembly has adopted cantonal laws on internal affairs, and the cantonal Ministries of Internal Affairs are responsible for implementing the laws of the canton which they belong to, as well as the laws and constitutions of the cantons and the Federation of Bosnia and Herzegovina in the field of internal affairs. The issue of conflict of jurisdiction between the Federal and Cantonal Ministries of Internal Affairs is also regulated in a way that the Federal Ministry supervises the implementation of federal laws and regulations whose enforcement is entrusted to the Cantonal Ministries of Internal Affairs (Ćeranić, 2023). The common link between the cantonal ministries and the Federal Ministry of Internal Affairs is a unified functional information and IT system, statistical data processing according to a standardised methodology, and a common database from the field of internal affairs based on electronic data processing (Miličević, 2023).

4.4. Police of the Brčko District of Bosnia and Herzegovina

The Police of Brčko District performs tasks within its jurisdiction on the territory of the district and, under the leadership of the Chief of Police, implements the security policy formulated by the Mayor and the Assembly of Brčko District (Ćeranić, 2023). In addition to the Chief of Police, the work of this internal affairs body is conducted through the following organisational units: Deputy Chief of Police, Assistant Chief of Police, Unit for Professional Standards, Operational Communication Center, Special Police Unit, General Police Unit, Traffic Police Unit, Unit for Investigating War Crimes, Unit for Preventing and Combating Terrorism and Extreme Violence, Criminal Police Unit, Unit for Administrative-Financial, Technical Affairs and Logistics.

Some of the responsibilities of the Brčko District Police regarding the protection of critical infrastructure include officer and patrol activities, securing facilities that are specially protected on the territory of Brčko District, inspection supervision in the field of security, organising the development of a functional system of communication, exchange and protection of information with the institutions of Bosnia and Herzegovina and entities (Official Gazette of Brčko District of Bosnia and Herzegovina, No 31/09, 60/10, 31/11, 14/19, 18/20, 41/20).

Police work in the security sector, officer and patrol activities in Bosnia and Herzegovina are conducted by the Police of Republika Srpska, Cantonal Police and the Brčko District Police, while this type of activity is not carried out by police bodies within the Ministry of Security of Bosnia and Herzegovina. The aforementioned activities of the police are important measures for the prevention of crime, disruption of public order and peace, and the

presence of the police also has a preventive effect on the safety of critical infrastructure. The existence of critical infrastructure facilities in the station area is one of the determinants based on which the patrol area (surface) is determined.

4.4. Other entities of the security system from the aspect of critical infrastructure protection in Bosnia and Herzegovina

Civil protection organisations are indispensable entities of critical infrastructure security. Civil protection in Bosnia and Herzegovina is organised through the Civil Protection Administration of Republika Srpska, the Civil Protection Administration of the Federation of Bosnia and Herzegovina, the Department for Public Safety of the Brčko District of Bosnia and Herzegovina, whereas the Ministry of Security of Bosnia and Herzegovina houses the Operational Communication Center 112. Civil protection tasks in Republika Srpska is performed by the Administration and Civil Protection Services in cities/municipalities. The Administration develops a civil protection programme, a risk assessment and a civil protection plan for the entire territory of Republika Srpska. Civil protection services in cities/municipalities perform these tasks at the local level, and upon the proposal of these services the mayor/head can approve organising specialised civil protection units for fire protection, flood protection, first medical aid, protection and rescue from unexploded ordnance and mines, radiological-chemical-biological protection, protection and rescue from the ruins as well as the terrain sanitation (Ćeranić, 2023). In the Federation of Bosnia and Herzegovina, in addition to the Federal Administration, there are also cantonal civil protection administrations and municipal civil protection services. The Federal Administration of Civil Protection prepares a risk assessment, develops program for protection and rescue from natural and other disasters, and proposes a plan for protection and rescue from natural and other disasters for the entire territory of the Federation of Bosnia and Herzegovina. It also organises and implements fire protection tasks and fire fighting, as well as training for headquarters and civil protection staff. All the aforementioned tasks at the cantonal level are performed by the cantonal civil protection administrations, while the civil protection services implement these tasks at the municipal level (Ćeranić, 2023). Planning for fire protection, accidents and other emergencies, demining, removal and destruction of unexploded ordnance, mines and explosives, monitoring and reporting in Brčko District is carried out by the Department for Public Safety of the Brčko District of Bosnia and Herzegovina (Ćeranić, 2023).

In addition to numerous entities at the entity level, the Armed Forces of Bosnia and Herzegovina constitute a unified military formation on the entire territory of the country. In the

context of critical infrastructure security, facilities of importance for the defense of the country are specially protected and it is expected that vital defense and military facilities, systems and buildings will remain under the authority of the defense regulations, rather than subject to laws on critical infrastructures directly. On the other hand, among the tasks of the Armed Forces of Bosnia and Herzegovina of interest for this dissertation are the fight against terrorism, the provision of military defense to the country and its citizens in the event of an attack, assistance to civil authorities in responding to natural and other disasters and accidents, and demining activities (Official Gazete of Bosnia and Herzegovina, 88/05). Activities in cases of natural disasters are precisely defined within the competence of the Department for Civil-Military Operations. Appendix 3 shows a tabular overview of 2052 successfully implemented activities of the Armed Forces of Bosnia and Herzegovina in the field of assistance to civil authorities for infrastructure recovery and rescue in special circumstances during 2019, 2020 and 2021 (Report on the work of the Ministry of Defense of Bosnia and Herzegovina for 2019, 2020, and 2021).

The Law on the Intelligence-Security Agency of Bosnia and Herzegovina defines that the Agency is responsible for collecting, analysing and distributing intelligence data related to threats to the security of Bosnia and Herzegovina. It timely informs the Presidency of Bosnia and Herzegovina, the Chair of the Council of Ministers of Bosnia and Herzegovina, the Minister of Foreign Affairs and the Minister of Defense of Bosnia and Herzegovina, the Presidents, vice-presidents and prime ministers of the entities, the ministers of internal affairs of the entities, the Chair and Deputy Chair of the House of Representatives of the Parliamentary Assembly of Bosnia and Herzegovina, the Chair and Deputy Chair of the House of Peoples of the Parliamentary Assembly of Bosnia and Herzegovina, the Chair and Deputy Chair of the National Assembly of Republika Srpska, the Chair and Deputy Chair of the House of Representatives of the Federation of Bosnia and Herzegovina, the Chair and Deputy Chair of the House of Peoples of the Federation of Bosnia and Herzegovina, as well as the Joint Commission for Supervision of Work of Intelligence and Security Agency of Bosnia and Herzegovina on matters of interest. In order to provide protection to institutions and facilities of special importance in the entire territory of Bosnia and Herzegovina, the Agency uses its operational means and methods. However, it is not responsible for providing physical protection to institutions and facilities (Official Gazette of Bosnia and Herzegovina, 12/04, 20/04, 56/06 and 12/09).

In addition to conventional entities of the security system, non-conventional elements of the security system also participate in the protection of critical infrastructure. Some institutions that were not presented on the previous pages should, in accordance with their competences and sectors of their operation, take part in the organisation of the resilience of critical infrastructure in Bosnia and Herzegovina. For example, in the energy sector, some institutions could include the State Electricity Regulatory Commission, Independent System Operator, Ministry of Energy and Mining of Republika Srpska, Federal Ministry of Energy, Mining and Industry.

Sectors from the Annex of the Directive 2022/2557	**Institutions of Bosnia and Herzegovina**	**Institutions of Republika Srpska**	**Institutions of the Federation of Bosnia and Herzegovina**	**Institutions of the Brčko District of Bosnia and Herzegovina**
Energy	− State Electricity Regulatory Commission − Independent System Operator	− Ministry of Energy and Mining	− Federal Ministry of Energy, Mining and Industry	

Table 4.3: Proposal of security entities in the field of critical infrastructure in Bosnia and Herzegovina for the energy sector [39]

Sectors from the Annex of the Directive 2022/2557	**Institutions of Bosnia and Herzegovina**	**Institutions of Republika Srpska**	**Institutions of the Federation of Bosnia and Herzegovina**	**Institutions of the Brčko District of Bosnia and Herzegovina**
Transport	− Ministry of Communications and Transport − Agency for the Provision of Air Navigation Services − Agency for Postal Traffic − Regulatory Board of Railways	− Ministry of Transport and Communications − Traffic Safety Agency	− Federal Ministry of Transport and Communications	

Table 4.4: Proposal of security entities in the field of critical infrastructure in Bosnia and Herzegovina for the transport sector [40]

[39] Source: Author's creation.
[40] Source: Author's creation.

Public security entities in the transport sector in Bosnia and Herzegovina are: Ministry of Communications and Transport of Bosnia and Herzegovina, Ministry of Transport and Communications of Republika Srpska, Federal Ministry of Transport and Communications, Agency for the Provision of Air Navigation Services, Agency for Postal Traffic of Bosnia and Herzegovina, Regulatory Board of Railways of Bosnia and Herzegovina, Traffic Safety Agency of Republika Srpska.

Sectors from the Annex of the Directive 2022/2557	**Institutions of Bosnia and Herzegovina**	**Institutions of Republika Srpska**	**Institutions of the Federation of Bosnia and Herzegovina**	**Institutions of the Brčko District of Bosnia and Herzegovina**
Banking	− Deposit Insurance Agency	− Banking Agency of Republika Srpska − Investment Development Bank of Republika Srpska	− Banking Agency of the Federation of Bosnia and Herzegovina	
Financial market infrastructure	− Ministry of Finance and Treasury − Ministry of Foreign Trade and Economic Relations − Indirect Taxation Authority − Insurance Agency in Bosnia and Herzegovina	− Ministry of Finance − Ministry of Economy and Entrepreneurship − Ministry of Trade and Tourism − Tax Administration − Foreign Exchange Inspectorate − Agricultural Payment Agency − Central Register of Securities ad Banjaluka − Securities Commission of Republika Srpska	− Federal Ministry of Finance − Federal Ministry of Trade − Federal Ministry of Development, Entrepreneurship and Crafts − Securities Registry in the Federation of Bosnia and Herzegovina	− Directorate for Finance − Office for the Audit of the Financial Operations of the Brčko District − Securities Commission

Table 4.5: Proposal of security entities in the field of critical infrastructure in Bosnia and Herzegovina for the banking and finance sectors [41]

The following public entities stand out in the banking and finance sectors: Deposit Insurance Agency of Bosnia and Herzegovina, Banking Agency of Republika Srpska, Investment Development Bank of Republika Srpska, Banking Agency of the Federation of Bosnia and Herzegovina, Ministry of Finance and Treasury and Ministry of Foreign Trade and Economic Relations in the Council of Ministers of Bosnia and Herzegovina. There are also republic ministries of finance, economy and entrepreneurship, trade and tourism, as well as the Tax Administration of Republika Srpska, Foreign Exchange Inspectorate, Agricultural

[41] Source: Author's creation.

Payment Agency, Central Register of Securities ad Banjaluka, and Securities Commission of Republika Srpska. In the Federation of Bosnia and Herzegovina, the relevant ministries for finance, trade, development, entrepreneurship and crafts stand out, as well as Securities Registry in the Federation of Bosnia and Herzegovina. The Directorate for Finance, Securities Commission and the Office for the Audit of the Financial Operations of the Brčko District Institutions are public entities of interest in the banking and finance sectors of the Brčko District of Bosnia and Herzegovina.

Sectors from the Annex of the Directive 2022/2557	**Institutions of Bosnia and Herzegovina**	**Institutions of Republika Srpska**	**Institutions of the Federation of Bosnia and Herzegovina**	**Institutions of the Brčko District of Bosnia and Herzegovina**
Health	− Agency for Medicinal Products and Medical Devices	− Ministry of Health and Social Welfare	− Federal Ministry of Health	− Department of Health and Other Services
Drinking water		− Ministry of Agriculture, Forestry and Water Management	− Federal Ministry of Agriculture, Water Management and Forestry	− Department of Agriculture, Forestry and Water Management
Waste water				− Department of Communal Affairs
Production, processing and distribution of food	− Food Safety Agency	− Ministry of Agriculture, Forestry and Water Management	− Federal Ministry of Agriculture, Water Management and Forestry − Federal Agro-Mediterranean Institute − Federal Institute for Agriculture − Federal Institute for Agropedology	− Department of Agriculture, Forestry and Water Management

Table 4.6: Proposal of security entities in the field of critical infrastructure in Bosnia and Herzegovina for the food and water sectors [42]

[42] Source: Author's creation.

The Agency for Medicinal Products and Medical Devices of Bosnia and Herzegovina, the Ministry of Health and Social Welfare of Republika Srpska, the Federal Ministry of Health, and the Department of Health and Other Services of Brčko District are public entities in the health sector, while entity ministries and departments of agriculture, forestry, water management and communal affairs in Brčko District are public entities in the sectors for drinking and wastewater. The responsibilities concerning the production, distribution, quality and food safety fall under the competence of the state Food Safety Agency.

Sectors from the Annex of the Directive 2022/2557	**Institutions of Bosnia and Herzegovina**	**Institutions of Republika Srpska**	**Institutions of the Federation of Bosnia and Herzegovina**	**Institutions of the Brčko District of Bosnia and Herzegovina**
Digital infrastructure		- Agency for Information and Communication Technologies		
Public administration	- General Secretariat of the Council of Ministers - Agency for Identification Documents, Records and Data Exchange	- General Secretariat of the Government of Republika Srpska	- General Secretariat of the Government of the Federation of Bosnia and Herzegovina - Ministries of all cantons	- Mayor's Office - Department of Public Affairs - Office for Public Property

Table 4.7: Proposal of security entities in the field of critical infrastructure in Bosnia and Herzegovina for the sectors of digital infrastructure and public services [43]

In the public services sector, notable entities include the General Secretariat of the Council of Ministers of Bosnia and Herzegovina, general secretariats of entity governments and ministries of all cantons in the Federation of Bosnia and Herzegovina, as well as the Mayor's Office, the Office for Public Property and the Department of Public Affairs in the Brčko District of Bosnia and Herzegovina. In the digital infrastructure sector, there is the Agency for Information and Communication Technologies of Republika Srpska which also includes the CERT of Republika Srpska. Currently, similar bodies have not been formed in another entity, Brčko District, nor at the level of the institutions of Bosnia and Herzegovina.

In addition to the proposed critical infrastructure security entities in each of the sectors provided for in Directive 2022/2257 (except for the space research sector for which there are no entities in Bosnia and Herzegovina), Table 10 lists other public entities/institutions that are

[43] Source: Author's creation.

important for Bosnia and Herzegovina and it is possible that domestic laws on critical infrastructure will have an expanded sectoral framework or prescribe sub-sectors where the mentioned institutions can be accommodated.

	Institutions of Bosnia and Herzegovina	**Institutions of Republika Srpska**	**Institutions of the Federation of Bosnia and Herzegovina**	**Institutions of the Brčko District of Bosnia and Herzegovina**
Additiona national sectors	− Ministry of Civil Affairs − Communication Regulatory Agency − Veterinary Office − Market Surveillance Agency − Institute for Intellectual Property	− Ministry of Administration and Local Self-Government − Ministry of Education and Culture − Ministry of Scientific and Technological Development and Higher Education − Ministry of Spatial Planning, Construction and Ecology − Agency for Higher Education − Republic Pedagogical Institute − Building and Reconstruction Directorate − Institute for the Protection of Cultural-Historical and Natural Heritage − Archives of Republika Srpska	− Federal Ministry of Education and Science − Federal Ministry of Physical Planning − Archives of the Federation of Bosnia and Herzegovina − Federal Commodity Reserves Directorate	− Department for Spatial Planning and Property-Legal Affairs − Department for Education − Public Registry Department − Department for Economic Development, Sport and Culture

Table 4.8: Proposal of security entities in the field of critical infrastructure in Bosnia and Herzegovina [44]

In addition to exclusively public institutions, it is necessary to mention other entities that inevitably have to participate in building the resilience of critical infrastructure. These are primarily telecommunications operators in Bosnia and Herzegovina that offer services in the mobile telephony, fixed telephony, digital television, internet and data transmission. M:tel a.d. Banja Luka is a joint-stock company in Republika Srpska whose majority owner (65%) is

[44] Source: Author's creation.

Telekom Republike Srbije. BH Telecom dd Sarajevo and HTEronet dd Mostar are majority owned by the Federation of Bosnia and Herzegovina.

5. Private entities in the field of critical infrastructure security in Bosnia and Herzegovina

Cooperation with the private security sector stems from the requirements of competent state authorities, including the area of critical infrastructure security. In Bosnia and Herzegovina, private agencies that commercially offer physical and technical security services are predominantly represented. The established offers of these companies are physical protection, security of public gatherings, security of facilities, security of VIPs, video surveillance, anti-burglary systems, fire alarm systems, access control systems, etc.

Middle Point Electronics d.o.o. Sarajevo offers technical protection services with the use of digital image and sound recording systems, engineering in the field of communication systems, conventional radio communication systems, radio control and management systems SCADA (Middle point, 2024). This company provides security services to the Federal Statistics Institute.

The Sector Security provides integrated security system services, anti-burglary system, access control and video surveillance to the company Rudnik and Gacko Thermal Power Plant, a regional giant in the field of electricity production supplying the European Union market. The largest health institution in Republika Srpska, the University Clinical Center, also utilises the technical protection services of the Sector Security company (Sector Security, 2024).

Omega Security, a company founded in 2023 with headquarters in Banja Luka, is trying to gain its place in the market by offering security consulting services (Omega Security, 2024). Infinity Ads offers a document digitisation service and is accredited by the Archives of Republika Srpska. Some of their clients are the Agency for Medicinal Products and Medical Devices of Bosnia and Herzegovina, the Archives of the Tuzla Canton, and Republika Srpska Pension and Disability Insurance Fund (Infinity ADS, 2024).

Private companies in Bosnia and Herzegovina that offer security services are: BB Gard Security doo, Bugojno; Sword Security, Sarajevo; As Security, Zvornik; Cobra-Security, Tuzla; Flek security, Tuzla; Delta Security, Čitluk; “Alpha-Security” d.o.o. Banja Luka; Peran Security Systems, Istočno Novo Sarajevo; Elektroinstal, Ilidža; Konektor, Banjaluka; Bond, Banjaluka, etc.

Respondent number 6, who is employed within one of the private security entities, emphasises at the beginning of the conversation that he cannot speak precisely about his company's role in protecting critical infrastructure because critical infrastructure in Bosnia and Herzegovina has not been defined or officially designated. Although it would be logical to conclude that a hydroelectric or thermal power plant, which are on the list of entities receiving physical and technical security services, represent critical infrastructure, there is no document that officially designates them as such. He mentions that energy sector entities, in addition to hiring private security agencies for facility protection, generally have their own internal security services and fire departments, and that they conduct business risk assessments without the involvement of the private security sector. Allocating money for security is always an investment, and the approach in the energy sector is considered appropriate in the context of protecting critical infrastructure, whether publicly or privately owned. This method of protection is particularly important for large companies with several hundred employees. Despite the profit-driven motivation of the private security agency the respondent represents, he emphasises that business risk assessments, security incidents and infrastructure recovery are best understood by employees who are permanently employed in a given company and familiar with the entire process of production and service provision. On the other hand, the banking sector in Bosnia and Herzegovina is almost entirely reliant on private security agencies to meet the needs for physical and technical security. These agencies are also engaged for risk assessment and the handling of cash transactions. Furthermore, the security and protection of companies with fewer employees (under 100) is entirely managed by private security agencies.

6. Information security from the aspect of critical infrastructure protection in Bosnia and Herzegovina

The regulation of the European Union stipulates that by July 2026, a list of critical entities must be determined, and by April 17, 2025, a list of key and important entities as well as entities in accordance with the recommendations of Directive 2022/2555 on measures for a high common level of cyber security throughout the Union. Research on the security of critical infrastructure must inevitably address information security for several reasons, one of which is the obligation to apply prescribed information security measures to all critical entities designated in accordance with Directive 2022/2557 and the corresponding national legislation (NIS 2 Directive).

The existing regulation in Bosnia and Herzegovina is not aligned with the security challenges of the modern era and is not applicable in the context of cyber security. The

European Commission's report for 2023 stated that Bosnia and Herzegovina does not have a comprehensive assessment or policy framework to address hybrid threats and remains vulnerable to computer attacks. In 2022, several serious cyber attacks were directed at the institutions of Bosnia and Herzegovina, including the highest legislative body in the country. Therefore, and it is necessary to undertake a series of activities in terms of building social structures that will be more resilient to all forms of hybrid threats (Bosnia and Herzegovina 2023 Report, 2023: 130).

In June 2023, the Parliamentary Assembly instructed the Council of Ministers of Bosnia and Herzegovina to take additional measures to implement the information security management policy in the institutions of Bosnia and Herzegovina. The Ministry of Security is to undertake activities on the development of a strategic framework for cyber security and establish a Computer Emergency Response Team (CERT), while the Ministry of Communications and Transport of Bosnia and Herzegovina is to draft a proposal for the Law on Information Security of Bosnia and Herzegovina. In this aspect of security, compliance with the regulations of the European Union is also being monitored, more precisely the provisions of Directive 2022/2555 on measures for a high common level of cyber security throughout the Union (the so-called NIS 2 Directive).

The strategic framework for cyber security of Bosnia and Herzegovina is to be developed in collaboration with the entities in Bosnia and Herzegovina, and Republika Srpska took concrete steps in the last quarter of 2023. The Government of Republika Srpska established the Agency for Information and Communication Technologies of Republika Srpska whose legally defined goal is to ensure the systematic development and application of information and communication technologies and electronic administration in Republika Srpska, while the Agency's task is the standardisation, management and supervision of the development and the use of information and communication technologies. As an independent legal entity, the Agency is to implement the concept of information security in Republika Srpska at both strategic and operational level. Within the Agency, there is the Republic CERT and the Operational Center for Information Security which coordinate prevention and protection against computer security incidents on the Internet and other security risks to the information systems of the public administrative bodies and other natural and legal persons. The Agency is also responsible for matters related to the digital identities of the public administrative bodies, the provision of trust services, electronic representation and signature services to the public bodies, legal and natural persons, as well as expert verification and prior

approval of all projects and procurement of information and communication technologies for the needs of the Government of Republika Srpska (Official Gazette of Republika Srpska, 90/23).

Specific steps in terms of initiating legislative procedures or establishing competent authorities in the field of information security in the Federation of Bosnia and Herzegovina and Brčko District are not visible. Based on the statements of respondents interviewed during the research for the purposes of this doctoral dissertation, the formation of a joint working group of all levels of government in Bosnia and Herzegovina is underway with the aim of developing a strategic framework for information security. After the adoption of the envisaged framework, the enactment of legal acts and by-laws at the entity level, the level of the Council of Ministers of Bosnia and Herzegovina and in the Brčko District of Bosnia and Herzegovina is expected, as well as the establishment of CERTs.

7. Functioning of critical infrastructure protection in Bosnia and Herzegovina

Despite numerous legal and practical shortcomings, all respondents who participated in the research agree that the critical infrastructure in Bosnia and Herzegovina is not completely unprotected and unresilient. They claim that the critical infrastructure in the defense sector is physically and technically secured, regulated by the internal rules of the Armed Forces of Bosnia and Herzegovina. In the sectors such as energy, banking and finance, there are internal bodies and regulations as well. Thermal power plants and hydroelectric power plants in Bosnia and Herzegovina have their own physical and technical security services, detailed procedures for a swift return “on the grid” as soon as possible in the event of an interruption in the production and delivery of electricity, as well as organisational sectors in the company responsible for the preparation, development, and staff training and supervision over the implementation of adopted rules and procedures. For performing tasks at workplaces designated as high-risk by internal regulations, fairly strict medical examinations of workers are carried out, but not security checks for individuals. Respondents believe that harmonisation with the existing legal framework for the security of critical infrastructure in Republika Srpska and/or a new one that should be adopted at the level of the Federation of Bosnia and Herzegovina, Brčko District and the institutions of Bosnia and Herzegovina, would require minimal financial expenditures and adaptation of entities in the energy sector, particularly in the context of staff training for enhancing information security and exchanging information with other entities.

In almost all banks in Bosnia and Herzegovina, there is a part of foreign capital, and all banks do business with other countries both in the region and globally. Doing business with entities in the member states of the European Union implies the application of Union rules, such as the General Data Protection Regulation (GDPR), whose provisions have not been implemented into laws in Bosnia and Herzegovina (Sikimić, 2022a). In this regard, the banking sector is left to its own devices and engages and trains its own staff in internal security sectors without the support of the state in order to achieve competitiveness in the international market. The situation is almost identical with private companies in all social areas that market their products and services outside the territory of Bosnia and Herzegovina. Certain private companies request information about their employees from the security services, and it can be said that the rules and procedures in the private sector in Bosnia and Herzegovina are largely in line with the security standards of business operations and the resilience of critical entities in the European Union.

On the other hand, the state administration primarily and exclusively acts in accordance with domestic positive law, and in the process of harmonisation with the legal acquis of the European Union in the field of security, it is necessary to adopt new laws on information security, personal data protection and strengthening the resilience of critical entities.

Despite the emphasised role of the Ministry of Security and entity ministries of internal affairs in the process of developing a strategic and legal framework for the security of critical entities, these bodies are not the ones that can provide critical infrastructure in Bosnia and Herzegovina. Their role is to direct, coordinate and supervise, while critical infrastructure entities must implement prescribed measures and ensure efficient provision of their services. The appointment of a security coordinator or manager from among the employees of the specific critical infrastructure entity is cited as the best solution. Advocating for this approach is justified by the fact that an individual within the structure of an organisation understands best the organisation's goals and tasks, business procedures, service delivery, as well as the organisation's weaknesses. According to the respondents' opinions, large budget investments are not required for the implementation and practical application of modern regulations on critical infrastructure security in Bosnia and Herzegovina, except in the area of information and communication technologies and raising standards in the area of information security.

The complex administrative apparatus and political system directly influence the area of critical infrastructure security in Bosnia and Herzegovina. In this country, competences are divided between the common sovereign state and lower-level federal units. Sovereign authority

over the internal area of 49% of the state territory belongs to Republika Srpska, while the Federation of Bosnia and Herzegovina holds authority over 51% of the state territory, and the self-governing Brčko District covers 492 square kilometers. The Council of Ministers of Bosnia and Herzegovina, composed of nine ministries, is the most important holder of legislative initiative and directly responsible for law enforcement at the state level, while entity governments have the same role in their respective entities and the Brčko District Government at the District level. The legislative power belongs to the parliaments in all the mentioned levels of authorities, and the Office of the High Representative and its discretionary powers in Bosnia and Herzegovina should gradually disappear on the path between Dayton and Brussels. In such a complex state structure, the development of public policies in the field of critical infrastructure security facilitates the existence of unified guidelines (directives) from the European Union. In Republika Srpska, the area of critical infrastructure security is partially regulated by laws and by-laws from 2019 and 2021, but the prescribed solutions have not yet been implemented in practice. At other levels of authority and parts of the territory of Bosnia and Herzegovina, normative initiatives concerning the critical infrastructure security at the level of the institutions of Bosnia and Herzegovina and in the Federation of Bosnia and Herzegovina were only launched in 2023. All adopted and proposed normative solutions follow the guidelines of the European Union, while the implementation of the critical infrastructure security framework is a challenge that the country needs to overcome in the years to come.

CONCLUSIONS

The main problem being addressed is how to establish an effective framework for the security of critical infrastructure in Bosnia and Herzegovina, while at the same time complying with European Union regulations and respecting the characteristics of the constitutional and political system as well as the security system of Bosnia and Herzegovina. Theoretical and empirical research is directed in accordance with the set hypotheses, scientific and practical research goals.

The guidelines of the European Union addressed to the member states clearly and unambiguously indicate that in the modern context the protection of critical infrastructure is organised and implemented at the level of the member states, with the obligation to exchange information with other states. Two decades of security policy development in the field of critical infrastructure in the European Union have been analysed, with an emphasis on Directive 2008/114/EC and Directive 2022/2557. In the first chapter of the dissertation, the definition of critical infrastructure from 2008 is stated, emphasising that it refers to a property, system or part of it located in the member states and that endangering it would have a significant impact on the member states. The definition of services provided by critical entities from 2022 states that it involves a service crucial for vital social functions or the economic stability of a state. An integral part of both definitions is the national level, that is, national critical infrastructure. The second chapter analyses the guidelines of Directive 2022/2557, i.e. the prescribed obligations for the member states to ensure the smooth provision of key services by defining goals and priorities in national strategies for the purpose of strengthening the resilience of critical subjects, implementing the provisions of this document in national legislation, establishing national management framework, conducting risk assessments at the national level, and defining necessary measures and public policy framework for information exchange. Supervision and implementation, as well as eventual sanctions related to the security of critical infrastructure are also prescribed in national legislation. The first hypothesis states: *"The protection of critical infrastructure is organised and implemented primarily at the national level"*, and based on the above, it was confirmed. The research results were published in related publications.[45]

[45] Related publication: Sikimić M. (2021): Consequences of threatening critical infrastructure on national security: a factor for building legal and institutional capacities. In conference proceedings: *Critical infrastructure protection: state obligations and private security sector opportunities*, pp. 96-112. ISBN 978-99976-914-3-9.

The second hypothesis states: "The capacities and mechanisms of the security system determine the efficiency and functionality of critical infrastructure." According to this hypothesis and in line with one of the practical goals of the dissertation to examine the normative and constitutional characteristics of contemporary security systems from the perspective of critical infrastructure, the third chapter of the dissertation provides theoretical elaboration of conventional and non-conventional entities of the national security system, i.e. supplementary entities and the private security sector. The role of the highest authorities of the legislative power is reflected in the adoption of strategic and/or legal acts in the field of critical infrastructure, approving budgets and controlling implemented measures. The executive apparatus has the task of implementing the decisions of the legislator and organising the protection of critical infrastructure by adopting sub-legal guidelines and through a network of its administrative bodies. Police organisations enforce laws within their competence and, through regular services, constantly work to prevent all illegal actions that may endanger critical infrastructure.[46] In addition to direct police action and the application of the state coercion mechanisms in the executive power sectors, where the national police are organisationally located (within ministries of internal affairs), there are also points of contact for exchanging information on critical infrastructure. Authorities responsible for information protection are formed in some countries within their intelligence services, while others do so within their military formations and defense systems. On the other hand, civil protection organisations have centers for alerting, rescuing and evacuating the population in emergency situations, as well as disaster recovery and infrastructure rehabilitation, terrain clearance and decontamination of the terain. Since natural disasters do not know national borders, the importance of international exchange of information and best practices between civil protection organisations is emphasised. In order to establish cooperation and mutual solidarity, regional and international civil protection organisations have been established. Maintening communal order in certain sectors of critical infrastructure is the responsibility of local communities as supplementary security entities, while the management of physical-technical protection systems is mainly conducted through the private security sector. Among the national critical infrastructure, the infrastructure of European importance is determined. Disruptions in the operation of infrastructure often have a cascading effect and cross the borders of one country, and in this way the elements of the national security system appear as entities of security in the

[46] Related journal article: Sikimić M. (2022): Rethinking the Basic Police Training Policy in Bosnia and Herzegovina. *Contemporary military challenges*, 24 (4), pp. 49-61. DOI:10.33179/BSV.99.SVI.11.CMC.24.4.3

regional or international context.[47] Therefore, it can be stated that the second hypothesis has been confirmed, but it is necessary to state the limitations, that is, the potential direction of further research related to this hypothesis. Namely, the dissertation did not cover research nor can it be asserted with certainty from the presented analysis whether weaker or stronger elements of the national security system including their technical development and equipment, staffing and training, as well as other normative and organisational characteristics, directly and/or to a certain extent, affect the efficiency of critical infrastructure in providing key services.

In relation to the presented determinants of the security framework, the fourth chapter conducted a scientific analysis of the security system and security policy of Bosnia and Herzegovina from the aspect of critical infrastructure. The results of the analysis also confirmed the third hypothesis, which states: "The protection of critical infrastructure in Bosnia and Herzegovina is not sufficiently effective and needs to be improved by adopting new normative and institutional solutions." The complex normative and institutional sphere, outdated laws in critical sectors, and the capacities of the security system of Bosnia and Herzegovina make the existing framework for the security of critical infrastructure insufficiently effective and point to the need for its improvement. Bosnia and Herzegovina is an internationally recognised state with two entities and one district, with a division of jurisdiction between the sovereign state and federal units. Within the legislative branch of government, a total of four parliaments have been identified as competent to adopt legal frameworks in the field of critical infrastructure. At the executive level, responsibility for initiating legislative initiatives falls under four governments with a total of nine ministries at the state level, thirty-two ministries in the entities, eleven departments and one office in Brčko District, as well as a three-member presidency at the level of the institutions of Bosnia and Herzegovina, plus two presidents of the entities and the mayor of Brčko District of Bosnia and Herzegovina. Additionally, the Federation of Bosnia and Herzegovina is composed of ten cantons, each of which has its own legislative, executive and judicial powers. In accordance with the aforementioned state organisation, the country requires at least four legal solutions in the field of critical infrastructure, namely: at the level of the institutions of Bosnia and Herzegovina, at the entity level and in the Brčko District of Bosnia and Herzegovina. Currently, only one such law from 2019 is in force, in Republika Srpska, partially aligned with the

[47] Related journal article: Sikimić M. (2022): Security of European critical infrastructures outside the European Union: a review of the Western Balkans national laws. *Insights into regional development*, 4 (2), pp. 63-72. DOI 10.9770/IRD.2022.4.2(5)

European directive that has been repealed.[48] The draft law in the Federation of Bosnia and Herzegovina was withdrawn from the legislative procedure in 2023, and it was also prepared according to outdated European Union guidelines. Obsolete legal solutions have been identified in critical sectors of information technology, and the regulation on the personal data protection in Bosnia and Herzegovina is not aligned with the General Data Protection Regulation (GDPR).[49] This situation initially forced the banking and finance sector in Bosnia and Herzegovina to follow the regulations of other countries. In order to maintain competitiveness on the European market, more and more private companies in other sectors are adopting the solutions of the banking sector.[50] Finally, there is an understanding in Bosnia and Herzegovina that only security agencies should be responsible for the security of critical infrastructure. There is almost no visible engagement or interest of public institutions to participate in the consideration of proposals and initiatives for regulating this area, such as those from the sectors of agriculture, water management, public services, education, transportation and health. Even some members of the working groups for drafting laws and methodologies on critical infrastructure, who were contacted during the research, are not familiar with or do not understand the conceptual and practical importance of normative regulation and resilience of critical infrastructure. Only certain organisational units or even individuals from the Ministry of Security of Bosnia and Herzegovina, entity ministries of internal affairs and the Government of Brčko District, as well as members of the academic community are familiar with the issues in the field of critical infrastructure security in Bosnia and Herzegovina and are directly engaged in them. Representatives of these bodies are willing to discuss legislative initiatives and proposals, while the process of identifying and designating critical infrastructure has only begun on the territory of Republika Srpska. One of the challenges faced by authorities during institutionalisation and designation of security coordinators for critical infrastructure sectors in Republika Srpska is the lack of qualified, educated and interested personnel who are familiar with the basics of security and are in charge of developing sectoral measures within the competence of the public institutions they represent. The results of a recent study on the protection of critical infrastructure in Republika Srpska,

[48] Related publication: Sikimić, M. (2021): Contemporary Security Challenges of the National Critical Infrastructure in the Republic of Srpska In: E. M.,Priorova (eds.),"*Curent security issues*," Moscow, Russia: Moscow Region State University, pp. 25-46.

[49] Related publication: Sikimić, M., Čihorić, S. (2022): Data protection in Republika Srpska. In: E.M.Priorova (eds), „*Curent security issues*," Moscow, Russia: Moscow Region State University, pp. 53-64. (Foreign co-author).

[50] Related journal article: Sikimić M. (2022): The GDPR Implementation In Non-Member States of the European Union: The Case of Bosnia and Herzegovina. *European data protection law review*, 8 (2), pp. 273-277. DOI https://doi.org/10.21552/edpl/2022/2/14

which support the confirmation of the third hypothesis, are presented in 35 charts with textual comments and published in a monograph of national importance.[51] The private security sector has not been involved in the process of designating critical infrastructure in Republika Srpska, as its capacities will only be used later on.

The fourth hypothesis states: *"The security framework for strengthening the resilience of critical infrastructure in Bosnia and Herzegovina is being developed according to the guidelines of the European Union."* In the justification provided by the executive power in Republika Srpska and the Federation of Bosnia and Herzegovina which have initiated legislative initiatives in the field of critical infrastructure, the need to harmonise domestic legislation with the legal acquis of the European Union is emphasised. More precisely, the draft laws state that they were prepared according to the provisions of Directive 2008/114/EC. Prior to its adoption by the National Assembly of Republika Srpska, the compatibility of the draft Law on Critical Infrastructure Security in the Republic of Srpska with the acquis of the European Union was considered by the Ministry of European Integration and International Cooperation of Republika Srpska. During 2023, the Ministry of Interior requested other departments of the executive power to develop sectoral measures according to the guidelines of Directive 2022/2557. Representatives of the Ministry of Security of Bosnia and Herzegovina advocate for the implementation of Directive 2022/2557 into domestic legislation, and the opening of new chapters in negotiations demonstrates not only progress, but also the country's commitment to European integration. Based on the results of the content analysis of official documents and according to the statements of the respondents, it can be undoubtedly said that the fourth hypothesis was fully confirmed, and the research results were published in a journal article.[52]

At the same time, respecting the legal acquis of the European Union and the specificities of the state organisation of Bosnia and Herzegovina, it is first necessary to regulate the area of critical infrastructure in the country normatively, and then proceed with the institutionalisation of prescribed solutions. The framework for the security of critical infrastructure should begin with the adoption of three additional laws in this area and amendments to the existing law of Republika Srpska. One of the laws would regulate the situation at the level of the institutions

[51] Amidzić, G., Sikimić, M. (2024): *Critical Infrastructure Protection - State and perspectives in Republika Srpska*. University of Business Engineering and Management, Faculty of Law in Lukavica. Banjaluka, pp. 209-252. ISBN 978-99955-40-74-6

[52] Sikimić M. (2022): Security of European critical infrastructures outside the European Union: a review of the Western Balkans national laws. *Insights into regional development*, 4 (2), pp. 63-72. DOI 10.9770/IRD.2022.4.2(5)

of Bosnia and Herzegovina, without explicit territorial competence, while the other two would be territorially and effectively directed towards the Federation of Bosnia and Herzegovina and the Brčko District of Bosnia and Herzegovina. These laws should define critical sectors, responsible entities, responsible individuals, as well as the coordination and cooperation process that will be aligned with the guidelines from Directive 2022/2557. Such a solution would be in line with the characteristics, real needs and capabilities of the security system, including the official policies of the constituent nations in Bosnia and Herzegovina. In the following, there is a presentation of how the implementation of the proposed solution could look like in practice.

New scientific results

The main and central scientific contribution of the dissertation lies in the results obtained from the analysis of security policy and the national security system from the perspective and in the function of protecting critical infrastructure in democratically organised states. Using Bosnia and Herzegovina as an example, through the lens of a new research matrix, the issue of critical infrastructure security is delineated on one side by the ambitions of political authorities aimed at the country's membership in the European Union. On other side, constitutional, territorial and ethnic variables and constraints are established, as well as normative solutions and the institutional capacities of the security system in Bosnia and Herzegovina.

The membership and/or position of a country in supranational political organisations has been identified as a new issue in the field of critical infrastructure security, i.e. as a central determinant of a strategic national approach to critical infrastructure protection. This result is based on the analysis of strategic, parliamentary and legislative initiatives and solutions that mandate alignment with one of the prevailing models within the European Union. Additionally, it draws from official reports of the relevant EU bodies which are presented in the dissertation.

Conventional security entities, such as the ministries of security and internal affairs, have been identified as central actors within the executive power and the main pillars of direct critical infrastructure protection. Furthermore, the research findings on the roles of specialised parliamentary bodies, cyber security agencies, private security companies, local communities, municipal police, public services, legal entities and citizens in the context of critical infrastructure security highlighted their importance and opened the door for new research

topics. These topics focus on the actions and authorities of civil society, the non-state sector and supplemental security entities in the function of protecting critical infrastructure.

Guided by the general goal of creating a safer and more resilient region, the findings of the dissertation can form the basis for a strategy aimed at developing a tailored, effective and regionally acceptable framework for critical infrastructure security in Bosnia and Herzegovina, taking into account the country's constitutional and multiethnic characteristics.

Practical use of results and recommendations

Based on the results obtained through research and the development of the dissertation, the following steps and a model for critical infrastructure security in Bosnia and Herzegovina are proposed.

First, it is necessary to regulate the field of critical infrastructure normatively in such a way as to adopt the following legal acts:

- Law on Critical Infrastructure Security in the institutions of Bosnia and Herzegovina;
- Law on Critical Infrastructure Security in the Federation of Bosnia and Herzegovina;
- Law on Critical Infrastructure Security in the Brčko District of Bosnia and Herzegovina;
- Amendments to the Law on Critical Infrastructure Security in the Republic of Srpska.

In each of these laws, it is necessary to define critical entities at the institutional level to which the law applies, inter-entity critical entities and critical entities of European importance. Then propose the sectors from which critical entities, inter-entity and European critical entities will be determined, regulate the management of critical infrastructure, mandate risk analysis, responsible security entities, security coordinators, single points of contact and the coordination body for intrastate and international exchange of information on critical entities, handling protected data, security checks for persons coming into contact with data on critical infrastructure, supervision of law enforcement and penalty provisions.

The definition of critical infrastructure and essential services can be directly adopted from Directive 2022/2557, Article 2. Below, we propose possible definitions in the proposed legislative acts for Bosnia and Herzegovina.

- The unified list of sectors from which critical entities will be designated at all levels in Bosnia and Herzegovina should align with the list of sectors used to determine key entities in the context of information security. The proposed list of sectors is as follows:
  - Energy,
  - Transport,
  - Digital Infrastructure,
  - Public Administration,
  - Banking and Finance,
  - Health,
  - Food and Drinking Water,
  - Communal Infrastructure, Wastewater, Chemicals and Hazardous Materials,
  - Educational and Research Institutions,
  - Cultural and Natural Heritage.
- Critical entities at the level of Bosnia and Herzegovina's institutions can be defined as public or private entities with associated critical infrastructure within the territory of Bosnia and Herzegovina which provide one or more key services to at least one public entity at the level of Bosnia and Herzegovina's institutions.
- Critical entities in the Republic of Srpska can be defined as public or private entities with associated critical infrastructure within the territory of the Republic of Srpska which provide one or more key services to at least one authority of the Republic.
- Critical entities in the Federation of Bosnia and Herzegovina can be defined as public or private entities with associated critical infrastructure within the territory of the Federation of Bosnia and Herzegovina which provide one or more key services to at least one authority of the Federation.
- Critical entities in the Brčko District can be defined as public or private entities with associated critical infrastructure within the territory of the Brčko District

which provide one or more key services to at least one authority of the Brčko District.

The definition and protection of inter-entity critical infrastructures should follow the example of defining European critical infrastructures in such a way that they are infrastructures whose disruption in operation may have an impact in one of the entities, Brčko District and/or institutions of Bosnia and Herzegovina. Inter-entity critical infrastructures should be designated from the list of critical infrastructures at the appropriate level of institutions/entities, with the obligation of all levels of authority to agree on a uniform methodology for risk analysis and identification of inter-entity critical infrastructures. Critical entities of European importance should also be appointed from among the list of critical infrastructures in Republika Srpska, Federation of Bosnia and Herzegovina, Brčko District and at the level of institutions of Bosnia and Herzegovina, following the corresponding provisions of Directive 2022/2557.

Inter-entity critical entities can be defined as public or private entities with associated critical infrastructure within the territory of one of the entities or the Brčko District of Bosnia and Herzegovina which provide one or more key services whose interruption or disruption in delivery could lead to negative effects in the territory of another entity, the Brčko District of Bosnia and Herzegovina, the institutions of Bosnia and Herzegovina or any of the entities in the case of critical infrastructure located within the territory of the Brčko District of Bosnia and Herzegovina.

Critical entities of European significance are those entities that are designated as key subjects within the entities, the Brčko District or at the level of Bosnia and Herzegovina's institutions which provide one or more key services to at least six other countries.

Due to the characteristics of the territorial organisation of Bosnia and Herzegovina, it can be expected that the minimum number of critical infrastructures will not be of inter-entity significance, and that there will be a certain number of overlaps between inter-entity and European critical infrastructures.

Normative measures should be accompanied by institutionalisation measures in such a way that single points of contact for the exchange of information on critical infrastructures are established in the Ministry of Interior of Republika Srpska, the Police Administration of the Federation of Bosnia and Herzegovina, the Police of Brčko District and the Directorate for Coordination of Police Bodies of Bosnia and Herzegovina (for the level of institutions of Bosnia and Herzegovina). The coordination body for the exchange of information on critical

infrastructure in Bosnia and Herzegovina can be formed in the Ministry of Security of Bosnia and Herzegovina. Each of the aforementioned bodies will have the role of both intrastate and international points of contact for the exchange of information on critical infrastructure.

The proposed model is aligned with the constitutional and political characteristics of Bosnia and Herzegovina, the organisation and capacities of the security system at the state level and its subsystems in the entities and district, as well as with the legal acquis of the European Union.

References

Achillopoulou, D. V., Mitoulis, S. A., Argyroudis, S. A., & Wang, Y. (2020). Monitoring of transport infrastructure exposed to multiple hazards: a roadmap for building resilience. *Science of The Total Environment. 2020 Dec 1;746:141001. doi: 10.1016/j.scitotenv.2020.141001. Epub 2020 Jul 18. PMID: 32795756.*

Adam, D. (2024). Lethal AI weapons are here: how can we control them? *Nature*, 2024, PMID: 38653827. doi: 10.1038/d41586-024-01029-0

Alexandru, A., Vevera, V., & Ciuperca, E. M. (2019). National security and critical infrastructure protection. *International Conference KNOWLEDGE-BASED ORGANIZATION* Vol. 25 No.1, pp. 8-13. Sciendo. DOI: 10.2478/kbo-2019-0001

Alqudhaibi, A., Majed A., Abdulmohsan A., Sandeep J., and Konstantinos S. (2023). *Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations. Sensors* 23 (9), 4539. https://doi.org/10.3390/s23094539

America's cyber defense agency. (2023, March 27). Retrieved from Financial Services Secto: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector

Amidzić, G., & Sikimić, M. (2024). *Critical Infrastructure Protection - State and perspectives in Republika Srpska*. Banjaluka: University of Business Engineering and Management, Faculty of Law in Lukavica. ISBN 978-99955-40-74-6 (Original: Амиџић, Г., Сикимић, М. (2024). *Заштита критичне инфраструктуре – стање и пресрпективе у Републици Српској*. Универзитет за пословни инжењеринг и менаџмент, Правни факултет у Лукавици. Бањалука. ISBN 978-99955-40-74-6).

Ampratwum, G., Osei-Kyei, R., & Tam, V. W. (2022). A scientometric review of public-private partnership in critical infrastructure resilience. *World Building Congress* 2022, doi:10.1088/1755-1315/1101/5/052007.

Anglmayer, I. (2021). Implementation Appraisal: European critical infrastructure, Revision of Directive 2008/114/EC. EPRS | *European Parliamentary Research Service; Ex-Post Evaluation Unit*; PE 662.604 – February 2021.

Arandjelović, D. (2022). The Serbian Or The Serbian Orthodox Church as a Transnational Political Actor: A Case Study of Regime Change in Montenegro. *All Theses*. 3945. https://tigerprints.clemson.edu/all_theses/3945

Beiraghdar F, Momeni J, Hosseini E, Panahi Y, Negah SS. (2023). Health Crisis in Gaza: The Urgent Need for International Action. *Iranian Journal of Public Health* 52(12), pp. 2478-2483. doi: 10.18502/ijph.v52i12.14309.

Besenyő, J., & Gulyás, A. (2021). The effect of the dark web on the security. *Journal of Security and Sustainability Issues,* 11, pp. 103-121., https://doi.org/10.47459/jssi.2021.11.7

Besenyő, J., & Málnássy, A. (2022). Future expansion and prospects of Turkish defense industry. *Insights into Regional Development*, 4(2), pp. 10-21., https://doi.org/10.9770/IRD.2022.4.2(1)

Besenyo, J., Feher, A. (2020).Critical infrastructure protection (CIP) as new soft targets: Private security vs common security. *Journal of Security and Sustainability Issues* 3(1), pp 5-18.

Besenyő, J., Márton, K., Shaffer, R. (2021). Hospital Attacks Since 9/11: An Analysis of Terrorism Targeting Healthcare Facilities and Workers. *Studies in Conflict & Terrorism*, pp. 1-24., https://doi.org/10.1080/1057610X.2021.1937821

Biçakci, S. (2022). *Enabling NATO'S collective defense: critical infrastrucutre security and resiliency* (NATO COE-DAT Handbook 1). Strategic Studies Institute. In Carol V. Evans, Chris

Anderson, Malcom Baker, Ronald Bearse, Salih Biçakci, Steve Bieber, Sungbaek Cho, Adrian Dwyer, Geoffrey French, David Harell, Alessandro Lazari, Raymond Mey, Theresa Sabonis-Helf, and Duane Verner, *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)* (Carlisle, PA: US Army War College Press, 2022), https://press.armywarcollege.edu/monographs/955

Bland, M., Leggetter, M., Cestaro, D., & Sebire, J. (2021). Fifteen Minutes per Day Keeps the Violence Away: a Crossover Randomised Controlled Trial on the Impact of Foot Patrols on Serious Violence in Large Hot Spot Areas. *Cambridge Journal of Evidence-Based Policing* 5, pp. 93–11., https://doi.org/10.1007/s41887-021-00066-3

Böröcz, M. (2021). Critical infrastructure protection policy in the EU. *Strategic Impact* (3), pp. 46-61., DOI: 10.53477/1841-5784-21-15.

Bosnia and Herzegovina 2023 Report. (2023, February 19). Retrieved from European Neighbourhood Policy and Enlargement Negotiations (DG NEAR): https://neighbourhood-enlargement.ec.europa.eu/document/download/e3045ec9-f2fc-45c8-a97f-58a2d9b9945a_en?filename=SWD_2023_691%20Bosnia%20and%20Herzegovina%20report.pdf

Brader, A. (2024, April 8). *Hungary's Military National Security Service Dedicates Cyberspace Operations Centre for 21st-Century Challenges*. Retrieved from Hungarian Conservative: https://www.hungarianconservative.com/articles/current/hungary_military_national_security_service_cyberspace_operations_centre_dedication/

Brown, K. A. (2006*). Critical Path: A Brief History of Critical Infrastructure Protection in the United States*. Fairfax, Virginia: Spectrum Publishing Group, Inc. ISBN 978-0-913969-06-9, https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_CriticalPath.pdf

Bueger, C., Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble? *Marine Policy* 155 (2023) 105772, https://doi.org/10.1016/j.marpol.2023.105772.

Buheji, M., Al-Muhannadi, K. (2023). Mitigating risks of environmental impacts on Gaza - review of precautions & solutions post (2023 war). *International Journal of Advanced Research in Engineering and Technology (IJARET)* 14 (7), pp. 15-47. DOI: https://doi.org/10.17605/OSF.IO/2JMCP

Cherney, A. (2018). Police community engagement and outreach in a counterterrorism context. *Journal of Policing, Intelligence and Counter Terrorism,* 13(1), pp. 60-79., https://doi.org/10.1080/18335330.2018.1432880

Commander of the European Union Force in BiH. (2024, January 22). Retrieved from European Unipn Force in BiH Operation ALTHEA: https://www.euforbih.org/index.php/eufor-commander

Council of the European Union. (21 March 2022). *Strategic Compass for Security and Defence – For a European Union tha protects its citizens, values and interests and contributes to international peace and security.* Brussels.

Critical Infrastructure Sectors. (2023, February 16). Retrieved from Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/critical-infrastructure-sectors

Critical Infrastructure Sectors. (2023, March 15). Retrieved from America's cyber defense agency: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Cyber defence. (2024, February 7). Retrieved from North Altalntic Treaty Organization: https://www.nato.int/cps/en/natohq/topics_78170.htm

Cybersecurity. (2024, February 10). Retrieved from Sigurnosno-obavještajna agencija: https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/ (Original: *Kibernetička sigurnost*).

Ćeranić, P. (2020). *Security policy – occasions in Bosnia and Herzegovina*. Faculty of security sciences. Banjaluka. ISBN 978-99976-756-2-0 (Original: Ћеранић, П. (2020). Безбједносна политика – прилике у Босни и Херцеговини. Бањалука: Факултет безбједносних наука. ISBN 978-99976-756-2-0).

Ćeranić, P. (2023). Security systems and control issue. Banjaluka: Faculty of security science. ISBN 978-99976-805-1-8. (Original: Ћераннић, П. (2023). Системи безбједности и питање контроле. Бањалука: Факултет безбједносних наука. ISBN 978-99976-805-1-8).

De Felice, F., Baffo, I., & Petrillo, A. (2022). Critical Infrastructures Overview: Past, Present and Future. *Sustainability* 14, No. 4: 2233. https://doi.org/10.3390/su14042233

Decret no 2006-212 du 23 fevrier 2006 relatif a` la securite´ des activites d'importance vitale. (2006). Paris. https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006053323

Department for European Integration and International Cooperation (2024, February 19). Retrieved from Vlada Brčko distrikta BiH: https://eims.bdcentral.net/Content/Read/o-odjeljenju (Original: Odjeljenje za evropske integracije i međunarodnu saradnju).

Dimitrijević, D. (2022). EU strategic compass for security and defence. *European Union Legislation, No.* 77-78, pp. 327-347. DOI: https://doi.org/10.18485/iipe_ez.2022.21.77_78.20

Djukić, A., Vuletić, D. (2023). Organization of the defense system according to the concept of total defense on the example of Switzerland, Sweden and Serbia. *International issues* 75(4), pp. 621-647., DOi: https://doi.org/10.2298/MEDJP2304621D.

Mijalkovski, M., Đorđević, I. (2010). *The elusiveness of national power*. Belgrade: JP Official Gazette. ISBN 978-86-519-0715-2 (Original: Nijalkoviski, M., Ђорђевић, И. (2010). *Неухватљивост националне моћи*. Београд: ЈП Службени гласник. ISBN 978-86-519-0715-2).

Ejdus, F. (2012). *International security: theories, sectors and levels*. Belgrade: JP Official Gazette and Belgrade Center for Security Policy. ISBN 978-86-519-1236-1. (Original: Ejdus, F. (2012). *Međunarodna bezbednost: teorije, sektori i nivoi*. Beograd: JP Službeni glasnik i Beogradski centar za bezbednosnu politiku. ISBN 978-86-519-1236-1).

EU integrations. (2024, February 7). Retrieved from Reoublic of Srpska Government: https://vladars.rs/eng/vlada/Activities/eu_integrations/Pages/default.aspx

European Commission (2022). *Annex to the proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities*. Brussels.

European Commission. (2003). *Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC).* Brussels: Official Journal of the European Union L 124/36.

European Commission. (2004). *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism* /* COM/2004/0702 final */. Brussels.

European Commission. (2005). *Green Paper on a European Programme for Critical Infrastructure Protection COM/2005/576 final*. Brussels: European Commission.

European Commission. (2006). *European Programme for Critical Infrastructure Protection COM(2006) 786 final.* Brussels: European Commission.

European Commission. (2019). *Evaluation of Council Directive 2008/114 of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* Brussels.

European Commission. (2023, November 27). Retrieved from European Civil Protection and Humanitarian Aid Operations: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/emergency-response-coordination-centre-ercc_en

European Parliament and the Council. (2016). *European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/ EC*. Brusselss: Official Journal of the European Union L 119/1.

European Parliament the Council. (2019). *Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN).* Brusselss: Official Journal of the European Union L 135.

FBiH Government Office for European Integration. (2024, February 7). Retrieved from Government of Federation of Bosnia and Herzegovina: https://fbihvlada.gov.ba/en/ured-vlade-fbih-za-evropske-integracije

FBiH Government Office for Legislation and Alignment with the EU acquis. (2024, February 7). Retrieved from Government of Federation of Bosnia and Herzegovina: https://fbihvlada.gov.ba/en/ured-vlade-fbih-za-zakonodavstvo-i-uskladenost-sa-propisima-eu

Federal Office for Civil Protection FOCP, Swiss federal authorities. (2024, May 10). Retrieved from Organisation of the FOCP: https://www.babs.admin.ch/en/organisation-of-the-focp

Forca, B. (2019). Theoretical determination of the functions of the national security system. *Security,* pp. 41-69., DOI 10.5937/bezbednost1901040F.

Georgescu, C., & Tudor, M. (2015). Cyber Terrorism Threats to Critical Infrastructures NATO's Role in Cyber Defense," *Knowledge Horizons - Economics*, Faculty of Finance, Banking and Accountancy Bucharest,"Dimitrie Cantemir" Christian University Bucharest, vol. 7(2), pp. 115-118.

Government of Federation of BiH. (2024, February 21). DECISION on the appointment of the Working Group for the drafting of the Draft Law on the Protection of Critical Infrastructure in the Federation of Bosnia and Herzegovina. Retrieved from https://fbihvlada.gov.ba/hr/140-rjesenje-o-imenovanju-radne-grupe-za-izradu-prednacrta-zakona-o-zastiti-kriticne-infrastrukture-u-federaciji-bosne-i-hercegovine

Government Resolution on the National Program for Critical Infrostructure Protection (2008). 2080/2008 VI.30. Budapest.

Guàrdia Urbana de Barcelona. (2024, March 25). Retrieved from https://ajuntament.barcelona.cat/guardiaurbana/en

Hale, J. R. (2009). *Lords of the Sea: The Epic Story of the Athenian Navy and the Birth of Democracy.* Viking Adult. ASIN: B002WTC8R0.

House of the people - working bodies. (2024, February 15). Retrieved from Dom naroda: https://parlamentfbih.gov.ba/v2/bs/stranica.php?idstranica=3 (Original: Dom naroda - radna tijela).

Hungarian legislation - Act CLXVI/2012 on the identification, selection and protection of critical systems and installations (10 May 2024). Retrieved: https://nki.gov.hu/wp-content/uploads/2020/11/CIP-Act_2012_166.pdf

ICDO. (2023, November 27). Retrieved from ICDO: https://icdo.org/about-icdo/history.html

Infinity ADS. (2024, February 1). Retrieved from: https://infinityads.ba/klijenti/

Information Technology Sector. (2023, March 17). Retrieved from America's cyber defense agency: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/information-technology-sector

Jens, W., Galić, D., & Sekulić, T. (2023). Bosnia and Herzegovina and European Union Integration, The Constitutional Impact of Accession to the European Union. In M. Sahadžić, D. Banović, D. Barbarić, & G. Marković, *Citizens, Constitution, Europe: glossary of essential constitutional concepts in BiH* (pp. 457-461). Sarajevo: Faculty of Law. ISBN 978-9926-544-03-4

Jensen, C. J., McElreath, D. H., & Graves, M. (2018). *Intorduction to Intelligence Studies*; Second Edition. New York and London: Routledge. ISBN: 978-1-498-73834-7 (hbk), ISBN: 978-1-315-11688-4 (ebk).

Jović, B. (2019). The relationship between the legislature and the executive - the power of the parliament and the responsibility of the government. *Proceedings of the Faculty of Law in Niš*, No. 82, pp 265-282., DOI: 10.5937/zrpfni1982265J (Original: Jović, B. (2019). Odnos zakonodavne i izvršne vlasti - moć parlamenta i odgovornost vlade. *Zbornik radova Pravnog fakulteta u Nišu*, broj 82, 265-282., DOI: 10.5937/zrpfni1982265J).

Jurišić, D. (2021). Regulations and deficiencies regarding the training of the protection and rescue units in Bosnia and Herzegovina. *Journal of Security and Criminal Sciences*, 3(2), pp. 47-61., DOI: 10.5937/zurbezkrim2102047J.

Kadena, E., & Rajnai, Z. (2024). 5G Supply Chain: An overview of applications and challenges. *2024 IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics (SAMI*) (pp. 157-162). IEEE. DOI: 10.1109/SAMI60510.2024.10432858

Komarčević, M. (2018). *Introduction to Critical Infrastructure*. Belgrade: Academic thought. ISBN 978-86-7466-718-7 (Original: Komarčević, M. (2018). *Uvod u kritičnu infrastrukturu*. Beograd: Akademska misao. ISBN 978-86-7466-718-7).

Kovács, A. M., & Besenyő , J. (2023). Healthcare Cybersecurity Threat Context and Mitigation Opportunities. *Security Journal,* 4(1), pp. 83-101. DOI: 10.37458/ssj.4.1.6

Kovács, L. (2023, Novembar 18). *Critical Infrastructure Protection with military aid.* Retrieved from https://defence.hu/news/critical-infrastructure-protection-with-military-aid.html

Krasznay, C. (2024). The role of civilian cybersecurity companies in military cyber operations. *Military art and science*, (113)/2024, pp. 1-11., DOI: 10.2478/raft-2024-0001.

Kunić, P., & Karan, S. (2012). *Constitutional law*. Banja Luka: Faculty of Security and Safety. (Original: Куниħ, П., & Каран, С. (2012). *Уставно право*. Бањалука: Факултет за безбједност и заштиту).

Laws, draft. (2024, May 12). Retrieved from Federal Ministry of Interior Affairs: http://www.fmup.gov.ba/v2/propisi.php?idkat=1

Lazari, A. (2014). *European Critical Infrastructure Protection*. London, (eBook): Springer. ISBN 978-3-319-07497-9.

Lehto, M. (2022). *Cyber-Attacks Against Critical Infrastructure*. In: Lehto, M., Neittaanmäki, P. (eds) Cyber Security. Computational Methods in Applied Sciences, vol 56, pp. 3-42. Springer, Cham. https://doi.org/10.1007/978-3-030-91293-2_1

Leslau, O. (2010). The Effect of Intelligence on the Decisionmaking Process. *International Journal of Intelligence and Counterintelligence*, 23 (3), pp. 426-448., DOI: 10.1080/08850601003772687

Maigre, M. (2022). *NATO's Role in Global Cyber*. GMF The German Marshall Fund of the United States: Policy Brief. Available at: https://www.gmfus.org/sites/default/files/2022-04/Maigre%20-%20NATO%20-%20Geopolitics%20-%20Cyber%20-%20final.pdf

Maksimović, G. (2022). Concept of public-private parthership and critical infrastructure protection. *Discourse on critical infrastructure* (pp. 83-102). Doboj: BIC BL. ISBN 978-99976-945-1-5.

Matz, J. (2022). Arms exports and intelligence: the case of Sweden. *Intelligence and National Security*, *37*(5), 710–731. https://doi.org/10.1080/02684527.2022.2034318

McFate, C. (2019). *Mercenaries and War: Understanding Private Armies Today*. National Defense University Press. Washington, D.C.

MiddlePoint. (2024, February 1). Retrieved from: https://www.middlepoint.ba/bs/about_us

Midorović, S. D., & Sekulić, M. B. (2019). A new function of personal data in the light of the contract for the supply of digital content and digital services. *International Scientific Conference Legal Tradition and New Legal Challenges* (pp. 1147-1150). Novi Sad: University of Novi Sad Faculty of Law.

Mijalković, S. (2018). *National security*. Belgrade: Police Academy. ISBN 978-86-7020-328-0 (Original: Мијалковић, С. (2018). *Национална безбедност*. Београд: Криминалистичко-полицијска академија. ISBN 978-86-7020-328-0).

Mijalković, S., & Bajagić, M. (2023). Methodological Guidelines for Conceptual Divergence of Bioterrorism, Agroterrorism, Biosecurity and Agrosecurity. *Security,* pp. 65-86., DOI: 10.5937/bezbednost2301065M

Mijalković, S., & Popović, M. (2016). *Introduction to security studies - methodological-research and theoretical bases of security*. Belgrade: Criminal and Police Academy. ISBN 978-86-7080-336-5 (Original: Мијалковић, С., & Поповић, М. (2016). *Увод у студије безбедности - методолошко-истраживачке и теоријске основе безбедности*. Београд: Криминалистичко-полицијска академија. ISBN 978-86-7080-336-5).

Mijalković, S., Milošević, M., & Ćeranić, P. (2023). *Intelligence and security services.* Banja Luka: Faculty of Security Sciences. ISBN 978-99976-976-9-1 (Original: Мијалковић, С., Милошевић, М., & Ћеранић, П. (2023). *Обавјештајне и безбједносне службе*. Бањалука: Факултет безбједносних наука. ISBN 978-99976-976-9-1).

Miličević, M. (2023). *Human resources management of the Federal Police Administration of the Federation of Bosnia and Herzegovina*. Sarajevo: Master thesis at Faculty of Political Sciences, University of Sarajevo. (Original: Miličević, M. (2023). *Upravljanje ljudskim resursima Federalne Uprave policije Federacije Bosne i Hercegovine*. Sarajevo: Master rad na Fakulteut političkih nauka Univerziteta u Sarajevu).

Milidragović, D., Subošić, D., & Milić, N. (2019). Police Procedure for Handling Orders and Requests Issued by the Competent Authorities. *Journal of security and criminal sciences*, 1(1), pp. 9-24., DOI: 10.7251/ZBKEN1901011M

Military Security Agency. (2024, August 19). Retrieved from https://www.vba.mod.gov.rs/cir/275/poslovi-i-zadaci-275

Mlađan, D. (2015). *Security in emergencies*. Belgrade: Police Academy. ISBN 978-86-7020-309-9 (Original: Млађан, Д. (2015). *Безбедност у ванредним ситуацијама*. Београд: Криминалистичко-полицијска академија. ISBN 978-86-7020-309-9).

Nagy, R. (2023). Identification of Chromatographic Parameters for Blister Agents in The Low Diesel Oil Contamination. *Safety and Security Sciences Review*, 5(3), pp. 91-106.

Nagy, R., Boda, P. (2022). Security Policy and Social Challenges of Epidemics in Our Days. *Polgari vedelmi szeml*e XIV, 271-285.

Nagy, R., Sikimić, M., & Baškalo, D. (2023). Contemporary threats to national security and protection of critical infrastructure from the health sector in the Republic of Srpska. Proceedings of the III International Scientific Conference "*Contemporary Challenges and Threats to Security,*" pp.

83-92. ISBN: 9789997697639 (Original: Nagy, R., Сикимић, М., & Башкало, Д. (2023). Савремене пријетње националној безбједности и заштита критичне инфраструктуре из сектора здравства у Републици Српској. Зборник радова III међународне научне конференције „*Савремени изазови и пријетње безбједности,"* стр. 83-92. ISBN: 9789997697639).

National Gazette of the Republic of Croatia. (14/2024). *Law on cyber security*. (Original: Narodne novine Republike Hrvatske. (14/2024). Zakon o kibernetičkoj sigurnosti).

National Gazette of the Republic of Croatia. (No 82/15, 118/18, 31/20, 20/21 and 114/22). *Law on the Civil Protection System of the Republic of Croatia*. Zagreb.

Newbill, C. M. (2019). Defining Critical Infrastructure for a Global Application. *Indiana Journal of Global Legal Studies* 26(2), pp. 761-780. Available at: https://www.repository.law.indiana.edu/ijgls/vol26/iss2/11

Office of the Coordinator of Brčko District of BiH in the Council of Ministers. (2024, February 1). Retrieved from Council of Ministers of Bosnia and Herzegovina: https://www.vijeceministara.gov.ba/stalna_tijela/javne_reforme/default.aspx?id=10301&langTag=en-US (Original: *Kancelarija koordinatora Brčko distrikta BiH u Vijeću ministara*).

Official Gazete of Bosnia and Herzegovina. (88/05). *Law on Defense of Bosnia and Herzegovina*. (Original: Službeni glasnik Bosne i Hercegovine. (88/05). *Zakon o odbrani*).

Official Gazette of BiH, 75/16, 02/18 and 32/23. (n.d.). *The Decision on the procedure for aligning legislation of BiH with the EU acquis.*

Official Gazette of BiH. (5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09 i 103/09). *Law on Ministries and Other Bodies of Administration of Bosnia and Herzegovina*. (Original: Службени гласник Босне и Херцеговине. (5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09 i 103/09). *Закон о министарствима и другим органима управе Босне и Херцеговине*).

Official Gazette of Bosnia and Herzegovina. (12/04, 20/04, 56/06 and 12/09). *Law on Intelligence–security agency of Bosnia and Herzegovina*. (Original: Службени гласник Босне и Херцеговине. (12/04, 20/04, 56/06 and 12/09). *Заком о обавјештајно-безбјендосној агенцији Босне и Херцеговине*).

Official Gazette of Brčko District of Bosnia and Herzegovina. (31/09, 60/10, 31/11, 14/19, 18/20, 41/20). *Law on the Police of Brčko District of Bosnia and Herzegovina*. (Original: Службени гласник Брчко дистрикта БиХ. (31/09, 60/10, 31/11, 14/19, 18/20, 41/20). *Закон о полицији Брчко дистрикта Босне и Херцеговине*).

Official Gazette of FBiH. (81/14). *Law on Internal Affairs of the Federation of Bosnia and Herzegovina*. (Original: Службене новине ФБиХ. (81/14). *Закон о унутрашњим пословима Федерације Босне и Херцеговине*).

Official Gazette of Republic of Kosovo. (2018). *Law on critical infrastructure.* Priština:.

Official Gazette of Republic of Serbia. (2018). *Law on critical infrastructure.* Belgrade.

Official Gazette of Republic of Serbia. (No 87/2018). *Law on Disaster Risk Reduction and Emergency Management*. Belgrade.

Official Gazette of Republika Srpska . (No 58/19). *Law on critical infrastructure security in Republika Srpska.*

Official Gazette of the Republic of Croatia. (2013, 2022). *Law on critical infrastructures.* Zagreb.

Official Gazette of the Republic of Srpska. (No 121/12, 46/17 and 111/21). *Law on Protection and Rescue in Emergency Situations of Republika Srpska*. Banjaluka.

Official Gazette of the Republic of Srpska. (57/16, 110/16, 58/19, 82/19, 18/22 and 55/23). *Law on Police and Internal Affairs*. (Original: Службени гласник Републике Српске. (57/16, 110/16, 58/19, 82/19, 18/22 и 55/23). *Закон о полицији и унутрашњим пословима*).

Official Gazette of the Republika Srpska. (90/23). *Law on the Agency for Information and Communication Technologies*. (Original: Службени гласник Републике Српске. (90/23). *Закон о Агенцији за информационо-комуникационе технологије*).

Official Gazzete of Montenegro. (2019). *Law on Designation and Protection of Critical Infrastructure*. Podgorica.

Official Journal of the European Union L 185/1. (2021). *REGULATION (EU) 2021/836 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2021 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism* .

Official Journal of the European Union L 333/164. (2022). *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*. Strasbourg.

Official Journal of the European Union L 333/80. (2022). *DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).* Strasbourg.

Official Journal of the European Union, Vol 59. (2016). *Council Regulation (EU) 2016/369 of 15 March 2016 on the provision of emergency support within the Union.*

Official Monitor no. 757 of November 12, 2010, Romania. EMERGENCY ORDINANCE no. 98 of November 3, 2010on the identification, designation and protection of critical infrastructures. Available at: https://cncpic.mai.gov.ro/en/despre-noi/cadru-legal?language=en. Accessed. 10 May 2024

OHR. (2024, February 3). Retrieved from Office of the High Representative: https://www.ohr.int/en/

Omega Security. (2024, Febrauary 1). Retrieved from: https://omegabezbjednost.com/usluge/#bezbjedonosni-konsalting

Parliament of the Federation of Bosnia and Herzegovina - Committees. (2024, February 15). Retrieved from Parliament of the Federation of Bosnia and Herzegovina: https://predstavnickidom-pfbih.gov.ba/sr

Paterson, C., & Williams, A. (2019). What Future for Policing? Some reflections on the concept and purpose of policing and their implications for police reform in England and Wales. *International Journal of Law and Public Administration,* 2(1), pp. 12-22., doi:10.11114/ijlpa.v2i1.4158

Pilipović, M. (2019). The legal nature of the system of government in the Republika Srpska. *Yearbook,* No 41, pp. 119-141. DOI 107251/GOD1941119P

Presidential Decree 39/2011 of the Hellenic Republic concerning the greek legislation adjustment to the relevant EU Directive EC 2008/114 of the European Council., 2011. Retrieved from The Center for Security Studies (Kentro Meleton Asfaleias – KEMEA): https://kemea.gr/en/legislation/

Public order office: What powers does the authority have? (2024, March 25). Retrieved from Ordnungsamt: https://www.bussgeldkatalog.org/ordnungsamt/

Qose, S., Rajnai, Z., & Fregan, B. (2023). Blockchain Technology in Healthcare Industry: Benefits and Issues. *2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)* (pp. 171-176). IEEE. DOI:10.1109/SACI58269.2023.10158669

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, 25, pp. 125-138., https://doi.org/10.1016/j.ijcip.2019.03.003

Report on the work of the Ministry of Defense of Bosnia and Herzegovina for 2019. (No 06-03-6-633-1/20 from 11 February 2022). Sarajevo.

Report on the work of the Ministry of Defense of Bosnia and Herzegovina for 2020. (No 06-06-6-776-1/21 from 24 February 2021). Sarajevo.

Report on the work of the Ministry of Defense of Bosnia and Herzegovina for 2021. (No 06-03-6-307-9/22 form 18 February 2022). Sarajevo.

Rules of Procedure governing the EU-BiH SAPC. (2024, February 19). Retrieved from https://www.parlament.ba/data/dokumenti/pdf/vazniji-propisi/180621_RoP%20EU-BiH%20SAPC%20as%20agreed%20in%2012042021%20D-SEE%20meeting%20CLEAN%20without%20EP%20heading.pdf

Rumi, S. K., Shao, W., & Salim, F. D. (2020). Realtime Predictive Patrolling and Routing with Mobility and Emergency Calls Data. *Proceedings of the International AAAI Conference on Web and Social Media,* 14(1), pp. 964-968., DOI: https://doi.org/10.1609/icwsm.v14i1.7367

Russel, S. (2023). AI weapons: Russia's war in Ukraine shows why the world must enact a ban. *Nature* 614(7949), pp. 620-623., DOI: 10.1038/d41586-023-00511-5

Schreier, S., & Leimbach, K. (2022). Same but different? A qualitative analysis of the influence of COVID-19 on law enforcement and organized crime in Germany. *Trends in Organized Crime* 26, pp. 180-201., https://doi.org/10.1007/s12117-022-09470-1

Sector for International Cooperation. (2024, January 26). Retrieved from Ministry of Security of Bosnia and Herzegovina: http://www.msb.gov.ba/onama/default.aspx?id=1661&langTag=en-US

Sector Security. (2024, February 1). Retrieved from Sector Security - Projects: https://sectorsecurity.org/sektor-projekti/

Sibalin, I., Cimer, Z., Kátai-Urbán, L., Szakál, B. (2020). Hungarian legal and institution system for critical infrastructure protection. *The science for population protection* 1/2020. Available at: http://www.population-protection.eu/prilohy/casopis/42/370.pdf. Accessed: 10 May 2024.

Sikimić, M. (2021): Contemporary Security Challenges of the National Critical Infrastructure in Republika Srpska. In: E. M., Priorova (eds.) *Curent security issues,* Moscow Region State University Moscow, Russia pp. 25-46. УДК: 351.865. Available at: https://www.elibrary.ru/item.asp?id=45840051&pff=1

Sikimić, M. (2022a). The GDPR Implementation In Non-Member States of the European Union: The Case of Bosnia and Herzegovina. *European Data Protection Law Review*, 8(2), pp. 273-277., DOI https://doi.org/10.21552/edpl/2022/2/14

Sikimić, M. (2022b). Consequences of threatening critical infrastructure on national security: a factor for building legal and institutional capacities. *Critical infrastructure protection - state obligations and private security sector opportunities* (pp. 96-112). Banja Luka: Research Center Banja Luka & Sector Security Banja Luka. ISBN 978-99976-914-3-9

Sikimić, M. (2022c). Security of European critical infrastructures outside the European Union: A review of the Western Balkans national laws. *Insights into regional development* 4(2), pp. 63-72., https://doi.org/10.9770/IRD.2022.4.2(5)

Sikimić, M., & Gnjatović, D. (2020). European Security Framework and critical infrastructure protection in the Republic of Srpska. *Security, police, citizens* 16(1-2), pp. 95-112., DOI 10.7251/BPGBL2001095S

Sikimić, M., Čihorić, S. (2022): Protection of personal data in Republika Srpska. In: E. M., Priorova (eds.) *Curent security issues,* Moscow Region State University Moscow, Russia, pp 53-64. Available at: https://www.elibrary.ru/item.asp?id=48523110&pff=1 (Original: Сикимић, М., Чихорић, С. (2022): Защита персональных данных в Республике Сербской. Сборник научных статей „*Актуальные проблемы безопасности.*“ Московский государственный областной университет, Москва, Россия, стр. 53-64. Доступно: https://www.elibrary.ru/item.asp?id=48523110&pff=1)

Simić, S., Jurišić, D., Maksimović, G., & Jovičić, R. (2020). *Fundamentals of critical infrastructure protection: critical infrastructure protection in Republika Srpska*. Doboj: Business and Technical College. ISBN 978-99976-945-2-2 (Original: Simić, S., Jurišić, D., Maksimović, G., & Jovičić, R. (2020*). Osnove zaštite kritične infrastrukture: zaštita kritične infrastrukture u Republici Srpskoj*. Doboj: Visoka poslovno tehnička škola. ISBN 978-99976-945-2-2).

Stanar, D. (2021). Peace as the purpose of the military. *A military act*, pp. 36-47., DOI: 10.5937/vojdelo2103036S (Original: Станар, Д. (2021). Мир као сврха војске. *Војно дело*, стр. 36-47., DOI: 10.5937/vojdelo2103036S).

Šljivić, D. (2021). Montenegro's Canonical Orthodox Church and Transition to Democracy in the Aftermath of the 2020 Parliamentary Elections. *Südosteuropa Mitteilungen* 61(1), pp. 47-61.

The BiH – EU Stabilisation and Association Parliamentary Committee. (2024, February 19). Retrieved from Parliamentary assembly of Bosnia and Herzegovina: https://www.parlament.ba/Content/Read/313?title=Parlamentarni-odbor-za-stabilizaciju-i-pridru%C5%BEivanje-izme%C4%91u-Parlamentarne-skup%C5%A1tine-BiH-i-Evropskog-parlamenta&lang=en

The Constitution of Bosnia and Herzegovina. (1995). Available at: https://www.ustavnisud.ba/public/down/USTAV_BOSNE_I_HERCEGOVINE_engl.pdf

The Council of the European Union. (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.* Brussels. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0:

The Council of the European Union. (2009). *Framework decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States.* Brusselss: Official Journal of the European Union L 93/23.

The Directorate for European Integration. (2024, February 19). Retrieved from The Directorate for European Integration: https://www.dei.gov.ba/en/o-nama

The Federal Administration of Civil Protection. (2024, May 10). Retrieved from https://www.fucz.gov.ba/nadleznost-uprave/

The National Assembly of Republika Srpska. (2024, February 15). Retrieved from: https://www.narodnaskupstinars.net/?q=ci

The National Directorate General for Disaster Management of the Ministry of Interior. Hungary. (2024, May 10). Retrieved from https://www.katasztrofavedelem.hu/2/bemutatkozas

The Military Intelligence Agency of Republic of Serbia. (2024, August 19). Retrieved from http://www.voa.mod.gov.rs/en/mia/competencies

The Report of the President's Commission. (1997). Critical Foundations - Protecting America's Infrastructures. Washington: http://www.fas.org/sgp/library/pccip.pdf.

The Republican Administration of Civil Protection of Republika Srpska. (2024, May 10). Retrieved from https://ruczrs.org/%d0%be-%d0%bd%d0%b0%d0%bc%d0%b0/

tportal. (2024, February 10). Retrieved from Zakon o kibernetičkoj sigurnosti uskoro pred Vladom: Evo šta sve donosi: https://www.tportal.hr/tehno/clanak/zakon-o-kibernetickoj-sigurnosti-uskoro-pred-vladom-evo-sto-sve-donosi-20230926

Trbojević, M. (2018). Critical infrastrucutre protection - experiences of transition countries. *Political revue* 2/2018, pp. 99-118., https://doi.org/10.22182/pr.5622018.5 (Original: Trbojević, M. (2018). Zaštita kritičnih infrastruktura - iskustva tranzicionih zemalja. *Politička revija 2/2018*, str. 99-118., https://doi.org/10.22182/pr.5622018.5).

Vlaški, B., & Davidović, M. (2023). The Entities in Bosnia and Herzegovina. In M. Sahadžić, D. Banović, D. Barbarić, & G. Marković, *Citizens, Constitution, Europe: glossary of essential constitutional concepts in BiH* (pp. 339-344). Sarajevo: Faculty of Law. ISBN 978-9926-544-03-4

Vranješ, N. (2020). Dayton and post-Dayton conception of the administrative authority of Bosnia and Herzegovina - twenty-five years after the Dayton Peace Agreement. *Politeia* 10(20), pp. 81-93., DOI: 10.5937/politeia0-29197 (Original: Vranješ, N. (2020). Dejtonska i postdejtnoska koncepcija upravne vlasti Bosne i Hercegovine - dvadeset i pet godina nakon Dejtonskog mirovnog sporazuma. *Politeia* 10(20), str. 81-93., DOI: 10.5937/politeia0-29197).

Vranješ, N., & Vlaški, B. (2023). The Brčko District. In M. Sahadžić, D. Banović, D. Barbarić, & G. Marković*, Citizens, Constitution, Europe: glossary of essential constitutional concepts in BiH* (pp. 355-359). Sarajevo: Faculty of Law. ISBN 978-9926-544-03-4

Watney, M. (2022). Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: a Legal Perspective. *European Conference on Cyber Warfare and Security* 21(1), pp. 319-327. DOI: 10.34190/eccws.21.1.196

Publications of the candidate

Publications of the candidate cited in the dissertation:

Nagy, R., Sikimić, M., & Baškalo, D. (2023). Contemporary threats to national security and protection of critical infrastructure from the health sector in the Republic of Srpska. Proceedings of the III International Scientific Conference *"Contemporary Challenges and Threats to Security,"* pp. 83-92., ISBN: 9789997697639 (Original: Nagy, R., Сикимић, М., & Башкало, Д. (2023). Савремене пријетње националној безбједности и заштита критичне инфраструктуре из сектора здравства у Републици Српској. Зборник радова III међународне научне конференције „*Савремени изазови и пријетње безбједности*," стр. 83-92., ISBN: 9789997697639).

Sikimic M. (2021): Consequences of threatening critical infrastructure on national security: a factor for building legal and institutional capacities. In conference proceedings: *Critical infrastructure protection: state obligations and private security sector opportunities*, pp. 96-112. ISBN 978-99976-914-3-9

Sikimić M. (2022): Rethinking the Basic Police Training Policy in Bosnia and Herzegovina. *Contemporary military challenges*, 24 (4), pp. 49-61. DOI:10.33179/BSV.99.SVI.11.CMC.24.4.3

Sikimić, M. (2022c). Security of European critical infrastructures outside the European Union: A review of the Western Balkans national laws. *Insights into regional development* 4(2), pp. 63-72., https://doi.org/10.9770/IRD.2022.4.2(5)

Sikimić, M. (2022a). The GDPR Implementation in Non-Member States of the European Union: The Case of Bosnia and Herzegovina. *European Data Protection Law Review*, 8(2), pp. 273-277., DOI https://doi.org/10.21552/edpl/2022/2/14

Sikimić, M., & Gnjatović, D. (2020). European Security Framework and critical infrastructure protection in the Republic of Srpska. *Security, police, citizens* 16(1-2), pp. 95-112., DOI 10.7251/BPGBL2001095S

Sikimić, M. (2021): Contemporary Security Challenges of the National Critical Infrastructure in Republika Srpska In: E. M., Priorova (eds.) *Curent security issues*, Moscow Region State University Moscow, Russia pp. 25-46. УДК: 351.865. Available at: https://www.elibrary.ru/item.asp?id=45840051&pff=1

Amidzić, G., & Sikimić, M. (2024). *Critical Infrastructure Protection - State and perspectives in Republika Srpska*. Banjaluka: University of Business Engineering and Management, Faculty of Law in Lukavica. ISBN 978-99955-40-74-6 (Original: Амицић, Г., Сикимић, М. (2024). *Заштита критичне инфраструктуре – стање и пресрпективе у Републици Српској*. Универзитет за пословни инжењеринг и менаџмент, Правни факултет у Лукавици. Бањалука. ISBN 978-99955-40-74-6).

Sikimić, M., Čihorić, S. (2022): Protection of personal data in Republika Srpska. In: E. M., Priorova (eds.) *Curent security issues*, Moscow Region State University Moscow, Russia, pp 53-64. Available at: https://www.elibrary.ru/item.asp?id=48523110&pff=1 (Original: Сикимић, М., Чихорић, С. (2022): Защита персональных данных в Республике Сербской. Сборник научных статей *„Актуальные проблемы безопасности*." Московский государственный областной университет, Москва, Россия, стр. 53-64. Доступно: https://www.elibrary.ru/item.asp?id=48523110&pff=1). (Foreign co-author).

Publications of the candidate not cited in the dissertation:

Sikimić M. (2021): African Relationships with the Military Industry of Bosnia and Herzegovina. *Journal of Central and Eastern European African Studies*, 1 (3), pp. 135-152.

Ćeranić P., Sikimić, M.: (2019): Energy security of Bosnia and Herzegovina. *Security, police, citizens*, 15 (3), pp. 3-17. DOI 10.7251/BPG1901003C

Ćeranić, P., Sikimić, M. (2018): Radicalization and violent extremism leading to terrorism. In conference proceedings „*Regional Cooperation in Fighting Transborder Crime: Contemporary Challenges of Terrorism and the Migrant Crisis*“, University of Banja Luka, Faculty od security sciences, pp. 33-46. УДК 323.28:321.64]:32.019.51

Ivanišević, M., Živak, N., Sikimić, M.: (2021): The treatment of natural hazards in municipal spatial plans in the Republic of Srpska. The 5th Serbian congress of geographers, *Innovative approach and perspectives of the applied geography* (Collection of Papers), pp. 186-196. ISBN 978-86-7031-589-1

Lalić, V., Ćeranić, P., Sikimić, M. (2019): Private and/or Corporate Security: Are There Conceptual Similarities and Differences? *Journal of security and criminal sciences* 1(1), pp. 51-65. DOI 10.7251/ZBKEN1901053L

Sikimić M.; Vujanović B. (2022): Bosnia and Herzegovina's Peacekeepers on African Soil during COVID-19: Procedures, Challenges, Lessons. *Journal of Central and Eastern European African Studies* 2 (4) pp. 137-145.

Sikimić, M, Lalić, V., Ćeranić, P. (2019): The Prevention of Radicalization, Violent Extremism, and Terrorism Through the Republika Srpska Education System. *Journal of security and criminal sciences* 1 (2), pp. 25-38. DOI 10.5937/zurbezkrim1902025S

Сикимић, М., Башкало, Д. (2023): Энергетическа безопасность Западных Балкан. Материалы VI Международной научно-практической конференции „*Современные региональные проблемы географии и экологии*“, Москва, Россия, стр. 163-173.

LIST OF FIGURES

LIST OF TABLES

APPENDIX

APPENDIX 1

THE QUESTIONNAIRE

In-depth interviews were based on the following questions:

- Q1: When did the activities in the area of critical infrastructure security start to be implemented in Bosnia and Herzegovina?
- Q2: Are the valid legal acts in the field of critical infrastructure in Bosnia and Herzegovina harmonized with the legal acquis of the European Union?
- Q3: Given the complex state regulation, which levels of government are responsible for the security of critical infrastructure in Bosnia and Herzegovina?
- Q4: What is the current situation in the area of critical infrastructure security in the entities and Brčko District of Bosnia and Herzegovina?
- Q5: Can the existing capacities of the security system of Bosnia and Herzegovina be the supporting pillars in the area of critical infrastructure security?
- Q6: Can you propose a model for organizing and implementing activities in the field of critical infrastructure in Bosnia and Herzegovina?

The results of the analysis are based on the answers of 9 respondents who were selected based on their relevance to the expertise, jobs, and tasks they perform on a professional or semi-professional basis in the field of critical infrastructure security and security policy. These include high-ranking officials of the Ministry of Security of Bosnia and Herzegovina, the Ministry of Interior of Republika Srpska, the CERT of Republika Srpska, the Government of the Federation of Bosnia and Herzegovina, the Government of Brčko District, of the private security sector, and of the scientific community.

APPENDIX 2

TABLE OF CONCORDANCE TEMPLATE

Creation date:	Identification number of the table			
CELEX number:	Title of BiH legal act:			
Title of EU legal act:				
1	2	3	4	5
Provisions of EU legal act	Reference	Provisions of BiH legal act	Conformity[53]	Remarks

[53] F = full conformity; P = partial conformity; N = not in conformity; N/A = non-applicable; NT = not-transposed

APPENDIX 3

THE 14 KEY PRIORITIES FOR OPENING EU ACCESSION NEGOTIATIONS AND OF THE STEPS SPECIFIED IN THE COMMISSION RECOMMENDATION FOR CANDIDATE STATUS OF BOSNIA AND HERZEGOVINA[54]

Key priority 1: Ensure that elections are conducted in line with European standards by implementing OSCE/ODIHR and relevant Venice Commission recommendations, ensuring transparency of political party financing, and holding municipal elections in Mostar.

Key priority 2: Ensure a track record in the functioning at all levels of the coordination mechanism on EU matters including by developing and adopting a national programme for the adoption of the EU acquis.

> *Step*: ensure a track record in the functioning at all levels of the coordination mechanism on EU matters including by developing and adopting a national programme for the adoption of the EU acquis.

Key priority 3: Ensure the proper functioning of the Stabilisation and Association Parliamentary Committee.

Key priority 4: Fundamentally improve the institutional framework, including at constitutional level, in order to: a) Ensure legal certainty on the distribution of competences across levels of government; b) Introduce a substitution clause to allow the State upon accession to temporarily exercise competences of other levels of government to prevent and remedy breaches of EU law; c) Guarantee the independence of the judiciary, including its self-governance institution (HJPC); d) Reform the Constitutional Court, including addressing the issue of international judges, and ensure enforcement of its decisions; e) Guarantee legal certainty, including by establishing a judicial body entrusted with ensuring the consistent interpretation of the law throughout Bosnia and Herzegovina; f) Ensure equality and non-discrimination of citizens, notably by addressing the SejdićFinci ECtHR case law; g) Ensure that all administrative bodies entrusted with implementing the acquis are based only upon professionalism and eliminate veto rights in their decision-making, in compliance with the acquis. NB: The June 2022 European Council called on the leaders of Bosnia and Herzegovina

[54] Available at: https://neighbourhood-enlargement.ec.europa.eu/document/download/e3045ec9-f2fc-45c8-a97f-58a2d9b9945a_en?filename=SWD_2023_691%20Bosnia%20and%20Herzegovina%20report.pdf pp: 9-13. Accessed: 2024, February 19.

to urgently finalise the pending constitutional and electoral reforms. These reforms should be advanced as an utmost priority.

Key priority 5: Take concrete steps to promote an environment conducive to reconciliation in order to overcome the legacies of the war.

Key priority 6: Improve the functioning of the judiciary by adopting new legislation on the 11 High Judicial and Prosecutorial Council and of the Courts of Bosnia and Herzegovina in line with European standards.

Step: adopt, as a matter of priority, integrity amendments in the existing law of High Judicial and Prosecutorial Council.

Key priority 7: Strengthen the prevention and fight against corruption and organised crime, including money laundering and terrorism, notably by: a) adopting and implementing legislation on conflict of interest and whistle-blowers' protection; b) ensuring the effective functioning and coordination of anti-corruption bodies; c) align the legislation and strengthen capacities on public procurement; d) ensuring effective cooperation among law enforcement bodies and with prosecutors' offices; e) demonstrating progress towards establishing a track record of proactive investigations, confirmed indictments, prosecutions and final convictions against organised crime and corruption, including at high-level; f) de-politicising and restructuring public enterprises and ensuring transparency of privatisation processes.

Step: adopt the Law on prevention of conflict of interest.

Step: take decisive steps to strengthen the prevention and fight against corruption and organised crime.

Key priority 8: Ensuring effective coordination, at all levels, of border management and migration management capacity, as well as ensuring the functioning of the asylum system.

Step: decisively advance work to ensure effective coordination, at all levels, of border management and migration management capacity, as well as ensuring the functioning of the asylum system.

Key priority 9: Strengthen the protection of the rights of all citizens, notably by ensuring the implementation of the legislation on non-discrimination and on gender equality.

Key priority 10: Ensure the right to life and prohibition of torture, notably by (a) abolishing the reference to death penalty in the Constitution of the Republika Srpska entity and (b) designate a national preventive mechanism against torture and ill-treatment.

Step: ensure prohibition of torture, notably by establishing a national preventive mechanism against torture and ill-treatment. **(The key priority is completed).**

Key priority 11: Ensure an enabling environment for civil society, notably by upholding European standards on freedom of association and freedom of assembly.

Key priority 12: Guarantee freedom of expression and of the media and the protection of journalists, notably by: (a) ensuring the appropriate judicial follow-up to cases of threats and violence against journalists and media workers, and (b) ensuring the financial sustainability of the public broadcasting system.

Step: guarantee freedom of expression and of the media and the protection of journalists, notably by ensuring the appropriate judicial follow-up to cases of threats and violence against journalists and media workers.

Key priority 13: Improve the protection and inclusion of vulnerable groups, in particular persons with disabilities, children, LGBTIQ persons, members of the Roma community, detainees, migrants and asylum seekers, as well as displaced persons and refugees in line with the objective of closure of Annex VII of the Dayton Peace Agreement.

Key priority 14: Complete essential steps in public administration reform towards improving the overall functioning of the public administration by ensuring a professional and depoliticised civil service and a coordinated countrywide approach to policy making.

APPENDIX 4:

ARMED FORCES OF BOSNIA AND HERZEGOVINA IN INCIDENT MITIGATION ACTIVITIES DURING 2019, 2020, AND 2021

Institutions	Number of requests to the Ministry of Defense of Bosnia and Herzegovina to undertake activities in emergencies			Number of approved/relized requests			Number of denied requests		
	2019	2020	2021	2019	2020	2021	2019	2020	2021
Institutions of government in Bosnia and Herzegovina	188	187	120	166	124	94	22	63	26
Law enforcement agencies	23	10	37	20	8	34	3	2	3
Educational institutions	22	7	17	20	7	15	2		2
Healthcare institutions		22	9		2	4		20	5
Churches and religious communities	36	11	12	32	8	10	4	3	2
International organizations	26	13	21	26	13	21			
Public companies	16	10	30	10	6	26	6	4	4
Companies	2	24	16		16	16	2	8	
Sports associations and clubs	42	36	35	28	16	20	14	20	15
Cultural and artistic societies	8		14	8		12			2
Fire Brigades									
Non-governmental organizations and associations of citizens	69	50	41	52	32	37	17	18	4
Military associations and veterans	250	93	141	247	91	139	3	2	2
Citizens	14	10	18	13	6	16	1	4	2
Other			1			1			
	696	473	512	622	329	445	74	144	67
∑	**1681**			**2052**			**285**		