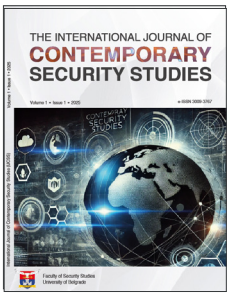
Volume 1 • Issue 2 • 2025 https://doi.org/10.18485/fb_ijcss.2025.1.2.15

Faculty of Security Studies, University of Belgrade

International Journal of Contemporary Security Studies (IJCSS)



Research article

Risks and Threats to Critical Infrastructure with Reference to Trends in the Protection of Critical Infrastructure in the Republic of Serbia

Steva Miletić[12*], Tamara Stojanović[1]

[1] Scientific-Professional Society for Disaster Risk Management, Dimitrija Tucovića 121, 11040 Belgrade, Serbia.

[2] ProSafeNet - Global Network Of Safety, Security, Risk & Emergency Professionals & Scientists.

[*] Correspondence: stevamiletic97@gmail.com.

Received: 17 September 2025; Accepted: 29 October 2025; Published: 30 December 2025.

ABSTRACT

Critical infrastructure consists of facilities, resources, and systems that are of vital importance for the functioning of a country's society and economy. Its importance is reflected both in regular and emergencies. Risks and threats are becoming increasingly frequent. In addition to their growing number, their destructive potential is also on the rise. A characteristic of the modern concept of critical infrastructure is the altered perception of risks and threats, as well as the increased interdependence between infrastructural elements. This influences the growing scope, content, and complexity of critical infrastructure, while potential threats pose a primary concern for national security. The forms of endangerment to critical infrastructure in this paper are divided into natural, external, and internal. The Republic of Serbia has undertaken the identification, determination, and protection of critical infrastructure. Like developed countries in this field, it is making efforts to address shortcomings in the normative and organizational framework. By adopting laws, bylaws, and appropriate strategies, a normative foundation has been established to support further development of the critical infrastructure protection system. The security and protection of critical infrastructure in the Republic of Serbia are conditioned by the relationship between threats and challenges, as well as by the ability to respond to them. In the final part of the paper, the normative and legal framework for critical infrastructure in the Republic of Serbia is analyzed, along with recommendations to improve the current state of protection.

KEYWORDS

Critical infrastructure; risks; threats; Republic of Serbia; normative-legal framework.

1. Introduction

By the end of the 20th century, critical infrastructure had become an important element of national security. At that time, critical infrastructure protection was introduced and has since become a priority for all states (Jakovljević, 2010). As a key segment of modern society, critical infrastructure faces a range of challenges and risks (Komazec, 2023). The challenges it encounters are numerous and complex. The growing number of hazards and threats creates an increasing need for adequate protection of critical infrastructure. In this context, protection

Miletic, S., & Stojanović, T. (2025). Risks and Threats to Critical Infrastructure with Reference to Trends in the Protection of Critical Infrastructure in the Republic of Serbia. International Journal of Contemporary Security Studies, 1(2), 203-214.

does not refer only to the infrastructure itself, but also to the consequences that may affect the economy and society. The functioning of the economy and society, both in regular and emergencies, is one of the primary and most important goals. This further initiates the development of a more resilient system in accordance with new requirements and more advanced technology. Successful prevention and emergency management are directly linked to an efficient critical infrastructure protection system (Komazec, 2023; Trbojević, 2018; Mićović, 2016). It is necessary to identify which infrastructure is critical to maintaining continuous services or functions and is vulnerable to specific threats or hazards. Prioritizing the allocation of resources to this group of infrastructure can improve security, increase resilience, and enhance long-term sustainability (Biringer, Vugrin, & Warren, 2013). Identifying hazards involves detecting and precisely describing all sources of danger and the scenarios in which they can occur. The result of identification is the prevention of undesired events and the prevention of the conditions that cause or worsen them (Cvetković, 2020). Resilience can be defined as the capacity of a system, the process through which the system is "strengthened," but also as a strategy for risk management (Ninković, 2024). The resilience of critical infrastructure is the ability to function under the influence of adverse external and internal factors (Lukas & Hromada, 2011).

The two terms "risk" and "threat," as key concepts of this paper, require closer definition. A security threat is considered anything that represents a source of danger and poses the potential to inflict serious harm on individuals, property, society, or the state (Mićović, 2020). Risk, on the other hand, refers to the combination of the probability that a disaster will occur within a specific period of time and the negative consequences associated with it.

Critical infrastructure refers to systems, services, and assets, whether physical or virtual, that are so vital to societal well-being that any disruption or destruction of these systems can have significant consequences for citizens' health, safety, and economic welfare, as well as for the effective functioning of government institutions (Košanin, 2018; Janković et al., 2025). It encompasses a wide range of sectors, including, but not limited to, the water supply sector, transportation and transit, energy production and distribution, information and communication technologies, healthcare, food supply, financial services, government institutions, and public administration (Rakić, 2015; Lewis, 2006; Jakovljević & Gačić, 2012).

Increasing operational complexities and growing interdependencies among systems have contributed to infrastructure vulnerabilities resulting from natural disasters, human errors, and technical failures. New forms of threats have also emerged, including cyber warfare, terrorism, and cybercrime. These events can have severe consequences, and in some cases, may lead to the destruction of infrastructure (Mićović, 2016). It is important to note that the term *"risk"* here refers to the combination of potential events and the likelihood of their consequences. In contrast, the term *"threat"* generally refers to harmful actions directed against infrastructure. *Vulnerability* can be defined as the degree to which a system, subsystem, or component is likely to be damaged by exposure to risks (Mićović, 2020).

The terrorist attacks on the USA on September 11, 2001, and the terrorist attacks in Paris, London, Moscow, Brussels, and Barcelona confirmed the need for a new approach to the protection of critical infrastructure. Likewise, natural disasters can have devastating consequences for infrastructure, such as hurricanes Katrina, Maria, and Irma, as well as tsunamis in Southeast Asia and Japan (Trbojević, 2018).

The Republic of Serbia is making considerable efforts to establish an integrated system of protection and rescue capable of effectively responding to threats to critical national resources (Jakovljević, 2010). However, a certain level of confusion can be observed regarding the security and protection of critical infrastructure. The first step in addressing this issue is to develop a comprehensive legal and normative framework to ensure the adequate protection of critical infrastructure. Although Serbia has enacted a Law on Critical Infrastructure, the sector is additionally regulated by numerous other legal acts, resulting in a degree of complexity and ambiguity in the field (Mladenović & Komazec, 2022; Cvetković & Stojković, 2015). From a normative-legal perspective, the Republic of Serbia adopted the Law on Critical Infrastructure in 2018. The domestic legal framework for the protection of critical infrastructure also includes a regulation defining the criteria for identifying critical infrastructure and the procedures for reporting on it. Furthermore, the Law on Public-Private Partnership represents one of the key instruments for the protection of critical infrastructure.

Trends toward the advancement and interconnection of all elements of critical infrastructure are underpinned by specific prerequisites, specifically specialized knowledge, which represents investments in preventive mechanisms that can be incorporated into the strategic framework for the protection of critical infrastructure.

In the future, the system for protecting critical infrastructure will be effective only through mutual understanding and coordination among state authorities, companies, and other stakeholders (Mićović, 2020).

The authors will use content analysis to collect domestic and international literature and to examine other research experiences, drawing on scientific papers, professional books, and journals. This method is also significant for studying normative-legal regulations by analyzing available and official laws, documents, and reports. The historical method will be used to examine past events to identify appropriate solutions for the future and to enhance responses to potential threats.

For this study, the authors will employ content analysis to collect domestic and international literature, as well as to examine other research experiences, drawing on scientific papers, professional books, and journals. This method is also significant for studying the normative-legal framework by analyzing available and official laws, documents, and reports. The historical method will be used to examine past events in order to identify appropriate solutions for the future and to enhance responses to potential threats.

The primary objective of this review paper is to present the risks and threats to critical infrastructure and clearly highlight the activities that should be undertaken to improve the functioning and protection systems of critical infrastructure in the Republic of Serbia.

2. Natural risks and threats to critical infrastructure as a form of vulnerability

Disasters caused by biological, hydrological, lithospheric, and climatic natural phenomena have become frequent occurrences in daily life. The consequences of these disasters often have destructive effects on life, health, material and cultural assets, as well as on the international community as a whole (Cvetković, Milojković, & Stojković, 2014; Cvetković & Filipović, 2017; Ocal, 2019).

Natural hazard-induced disasters are understood as events in which interactions occur between specific hazards (lithospheric, hydrospheric, atmospheric, biospheric, and extraterrestrial) and built social systems, resulting in consequences for community safety and normal functioning. This necessitates additional efforts to restore life and all other social activities to their previous "normal" state. Natural disasters can also be understood as the consequences of spatial interactions between hazardous ecological processes and the population, or specific vulnerable segments thereof (Cvetković, 2023; Cvetković, 2020, p. 84; Degg, 1992, p. 199; Cvetković & Stojković, 2015). According to the International Strategy for Disaster Reduction (ISDR, 2009), natural hazards are natural processes that cause losses in human life, health, and services, as well as disruptions to the economy and social protection, and lead to environmental degradation.

A significant increase in natural disasters causing serious consequences for critical infrastructure has been observed (Korajlić & Marjanović, 2022; Kaur, 2020). Broadly speaking, critical infrastructure can be affected or damaged by various natural phenomena, such as floods, earthquakes, strong winds, landslides, snowfalls, hail, and similar events. These changes lead to a growing number of catastrophic events, significantly increasing the need for forecasting, planning, and strengthening the system (Milenković, 2025).

The risk and threats from disasters caused by a single natural event are often accompanied by another natural phenomenon, or even a chain of events. An example of such a situation is the earthquake followed by a tsunami in Japan, which was subsequently accompanied by a series of accidents triggered by the earthquake, significantly affecting the functioning of critical infrastructure. The tsunami, triggered by the earthquake, affected nuclear power plants, reducing the total energy required for delivery to the consumer grid (Korajlić & Marjanović, 2022; Kumiko & Shaw, 2019; Onuma, Shin, & Managi, 2017). Subsequent seismic shocks can cause greater damage to already weakened structures (Cvetković & Planić, 2022). Secondary effects of earthquakes include fires, dam ruptures, and landslides, which can block land and water routes and cause flooding. Damage to facilities where hazardous materials are used or produced may result in chemical leaks.

Similarly, the earthquake that struck the Republic of Serbia and the city of Kraljevo on November 3, 2010, seriously endangered critical infrastructure. On that day, the city experienced heating issues and partial power outages, and water was deemed unsafe for drinking. The maternity ward was flooded, the operating rooms at

the "Studenica" Clinical Center were non-functional, and store shelves collapsed, severely disrupting the supply of goods to citizens (Mićović, 2016, p. 47).

Floods are by far the most frequent and dangerous threat, and, as a hazard, they can lead to erosion. Erosion, in turn, can undermine bridges, embankments, and buildings, eventually causing their collapse (Aktar et al., 2021; Korajlić & Marjanović, 2022; Perić & Cvetković, 2019). The 2014 floods primarily affected central and western Serbia. During this event, the Kolubara Mining Basin was also impacted. Due to flooding of the Kolubara River on May 15–16, 2014, mining equipment was submerged, and parts of the railway used to transport coal from the Kolubara mine were damaged. This resulted in a suspension of coal transport to Obrenovac. As a consequence, production was significantly reduced during the period from May 15 to May 25 (Miletić, 2023; Vlada Republike Srbije, 2014).

Strong storm winds can damage overhead power lines or telecommunications lines, which are considered critical infrastructure assets. Addressing the consequences of stormy weather in modern society requires an electricity supply; in this sense, critical infrastructure serves to provide quality medical care, food preparation, and other essential services. Communication and telephone systems are the lifeline of the protection and rescue system and, as such, depend on wired connections. Without them, the system must rely solely on radio communications, which can quickly become a "bottleneck" in any significant protection and rescue operation (Jakovljević, 2010, p. 65).

Awareness of the importance of the functioning of infrastructure systems—from the consequences of a destroyed bridge that disrupts the movement of resources and citizens within a community, to a major failure at a power plant during the winter months when electricity is a matter of life and death—represents a significant step toward effective risk and threat management of natural disasters (Cvetković, 2014).

To better understand the impact of natural disasters on critical infrastructure, it is essential to understand the fundamental qualitative and quantitative indicators of natural disasters at the global level and over longer periods. By analyzing statistical results on the geospatial and temporal distribution of various natural disasters (Cvetković & Mijalković, 2013; Cvetković, 2013), it is evident that natural disasters increasingly threaten people and their assets, including critical infrastructure.

3. External risks and threats to critical infrastructure as a form of vulnerability

One of the most severe forms of external risks to critical infrastructure is armed aggression. Depending on political, geopolitical, and military interests, armed aggression aims to bring about radical changes. Its ultimate objective is the occupation of territory and the destruction of the constitutional, economic, and social system of a state (Miletić, 2023; Stajić, 2015).

The increasing dependence of societies on information technologies leads to new forms of threats that these societies must be able to confront, whether they are intentional threats, anthropogenic in nature, or natural disasters. Such often recurring and sophisticated threats impact cyber, national, and international security. Cyber threats originate from various sources and manifest through disruptive activities targeting individuals, economic entities, and national infrastructure. They are characterized by specific features such as their transnational nature, the anonymity of attackers, dispersion, and the ability to strike from a distance without direct contact with the target. Threat actors can include individuals, states, or non-state entities. The main threats that modern nation-states face today include hacking, cybercrime, cyberterrorism, political and ideological extremism, cyber espionage, and state-sponsored cyber-attacks and aggression, i.e., warfare (Miletić, 2023; Ptáček & Skoruša, 2015). These events indicate a fundamental shift in the structure of modern conflicts (Vračević, 2025). Cybersecurity is essential for the sustainable growth of nations (Vidović & Beriša, 2025).

Today, terrorism poses a threat in many countries worldwide, ranking among the most pressing security risks of the present day (Pribičević, Janković, & Živković, 2022; Krstić, 2016). Infrastructure can easily become a target for terrorist organizations (Mančić, 2025). Terrorism constitutes one of the most significant challenges in ensuring security from a global, regional, and national perspective. As an international threat, it goes beyond the scope of traditionally defined conflicts and crises. The activities of terrorist organizations may specifically aim at reaching the media for propaganda purposes (gaining publicity for those who carried out the terrorist attack, creating a sense of societal insecurity, spreading ideology, and recruiting followers), achieving political

objectives (forcing state authorities to take or refrain from specific actions), as well as economic goals (causing economic problems or disruptions in securing the country's energy resources) (Miletić, 2023; Zubrzycki, 2017).

Terrorist activities may be carried out to destroy or turn off water, craft, hydraulic structures, and port facilities in order to take control over them. The objective of a terrorist act may also be to provoke an environmental disaster (ecoterrorism); an example of this is oil spills. In such cases, the targets of terrorist acts may include tankers, oil transshipment facilities, coastal installations, oil storage units, and offshore oil platforms. Terrorist attacks can target elements of port infrastructure, particularly those involving seaports and handling terminals, as well as military port facilities. Another group of potential targets includes hydraulic structures such as drilling platforms, pipelines, or underwater cables (Miletić, 2023; Zubrzycki, 2017).

Intelligence and reconnaissance activities can also be classified as external forms of endangerment, as they involve operations aimed at collecting necessary information. In traditional warfare, an adversary would attempt to gather as much information as possible before launching an attack. The goal is to learn about available resources, their weaknesses, and their vulnerabilities. Various methods may be used to obtain such information, including surveillance, eavesdropping, interception of communications, and initiating espionage investigations (Miletić, 2023; Shaikh et al., 2008).

The prevention of terrorist attacks, aggression, intelligence and reconnaissance activities, and cyber threats to critical infrastructure should be part of a broader national strategy. This strategy would focus on anticipating such attacks, detecting plans, conspiracies, and other activities, and disrupting and preventing them. In this context, the protection of critical infrastructure primarily depends on the coordinated activities of intelligence agencies, police, and other law enforcement authorities (Pribičević, Janković, & Živković, 2022).

4. Internal risks and threats to critical infrastructure as a form of vulnerability

Sabotage refers to individual or group activities aimed at causing harm to business enterprises (Mićović, 2016). Typically, when one thinks of sabotage, the image of someone breaking or physically destroying something comes to mind. However, sabotage is only contingently associated with a specific tactic that may be carried out in any given situation. Sabotage is a form of action that operates through circulation, transportation, and mobility infrastructure (Miletić, 2023; Barney, 2019).

It takes many forms, such as disruptions to the expansion of the oil economy, including physical blockades and the occupation of testing sites and pipeline routes, obstructive interventions in public debates and regulatory procedures, assertions of territorial sovereignty and stewardship, litigation, disputes, and licensing approvals. In this sense, sabotage is materialistic: it relies on a network of human and non-human agents, a confederation of workers, locations, architectures, machines, processes, and materials (Miletić, 2023; Barney, 2019).

Perpetrators of sabotage plan and execute all tasks very deliberately to avoid detection. Saboteurs can be individuals who infiltrate a system or those already employed within it, performing ordinary or managerial tasks and thus having access to targeted locations. The fundamental characteristic of sabotage lies precisely in the perpetrators' intimate knowledge of the system (Miletić, 2023; Mićović, 2016).

Crime is defined in multiple ways among experts in this field. It can refer to any deviant behavior, or it can be limited to unlawful conduct that is punishable as a criminal offense. Crime is, in fact, one of the most pressing issues in all modern countries, including our own, as evidenced by its continuous increase. Due to its social danger and harmfulness, all societies strive to suppress it—either preventively or repressively—by continually seeking more effective methods and means. In these efforts, there is a noticeable shift from primarily repressive measures toward preventive measures aimed at preventing crime (Stajić, 2015, p. 300).

In today's world, cyber threats can harm critical infrastructure, leading to service disruptions essential to sustaining life, catastrophic economic damage, or severe degradation of national security. Vulnerability to cyber threats has increased (Dada et al., 2025). The complexity and diversity of cyber threats exploiting vulnerabilities in critical infrastructure are growing daily. To minimize the potential damage from cyber threats, countermeasures must be implemented and their effectiveness continuously monitored (Miletić, 2023; Karabacak & Tatar, 2014).

First, it is necessary to determine the characteristics of the threat, as this will be useful for risk assessment. Risk prevention activities should be initiated by international and national organizations responsible for proposing and adopting laws and strategies, launching initiatives and programs, and defining legal frameworks to reduce the risk of such forms of endangerment within the relevant systems (Pribičević, Janković, & Živković, 2022).

5. Analysis of critical infrastructure from a normative-legal perspective and trends for improving the protection of critical infrastructure in the Republic of Serbia

In terms of legislation, the Republic of Serbia has made significant efforts in recent years. In 2018, the Law on Critical Infrastructure was adopted. The scope of this law (Službeni glasnik broj, 87/18) regulates national and European critical infrastructure, establishes its definition and identification, defines the competencies and responsibilities of authorities and organizations in the field of critical infrastructure, governs data protection, information provision, and reporting, as well as oversight implementation and management procedures.

The Regulation on the Criteria for the Identification of Critical Infrastructure and the Method of Reporting on Critical Infrastructure in the Republic of Serbia was adopted in 2022. This regulation (Službeni glasnik broj 69/22) establishes the criteria for identifying critical infrastructure, which are determined based on an assessment of the consequences that may arise from the disruption or destruction of critical infrastructure, as well as the potential consequences in the event of threats to it.

The sectors of critical infrastructure in the Republic of Serbia are: energy, transportation, water and food supply, healthcare, finance, telecommunications and information technologies, environmental protection, and the functioning of state authorities.

The National Security Strategy of the Republic of Serbia from 2019 states that the dynamics of global information technology development will lead to further intensification of activities in cyberspace, whose security will primarily be threatened by cyber espionage, attacks on critical infrastructure, unauthorized intrusions into classified databases, as well as the spread of fake news and disinformation through social networks (Službeni glasnik broj, 94/2019).

The same document notes that critical infrastructure facilities will be identified and protected, and early warning and preventive response measures will be implemented to address natural disasters, technological accidents, and catastrophes. It further states that climate change, along with the increasing scarcity of natural resources, is expected to lead to a rise in conflicts worldwide caused by competition for energy resources and other natural raw materials, as well as for drinking water and food. In addition, the increased risk of attacks on energy transport infrastructure will compel states to significantly strengthen the protection of critical energy infrastructure, including the use of military forces (Službeni glasnik broj, 94/2019).

The Defense Strategy of the Republic of Serbia from 2019 states that ensuring the security of critical infrastructure is of primary importance for protecting the security of the Republic of Serbia and its citizens. In this regard, the identification and protection of critical infrastructure facilities will be regulated by law and aligned with European Union regulations. Special attention will also be given to the full implementation of legal and normative measures. To ensure the security of critical infrastructure facilities, all preventive measures will be continuously undertaken, particularly regarding protection against fires, explosions, and terrorist attacks. An integrated information system for the security monitoring of critical infrastructure facilities will be established. For prevention, timely, and effective response to emergencies, functional integration of services relevant to protection, rescue, and emergency management will be ensured, along with the establishment of a public warning system across the territory of the Republic of Serbia. Measures will be taken to ensure continuous training for emergency headquarters and the population in performing protection and rescue tasks (Službeni glasnik broj 94/2019).

Based on the Law on Disaster Risk Reduction and Emergency Management (Službeni glasnik broj, 87/18), a Methodology for the Preparation and Content of Disaster Risk Assessment and Protection and Rescue Plans has been adopted (Mladenović & Komazec, 2022; Službeni glasnik broj, 80/19), which re-identifies critical fa-

cilities, critical locations, and areas from the perspective of vulnerability. According to the Methodology (Official Gazette No. 80/19), critical infrastructure consists of systems, networks, facilities, or their components, the disruption of which, or the interruption of the delivery of goods or services, may have serious consequences for national security, human health and life, property, the environment, citizen safety, economic stability, or may threaten the functioning of the Republic of Serbia. The following infrastructure has been identified:

1) Energy infrastructure includes: thermal and hydroelectric power plants, combined heat and power plants, and other electricity generation facilities, as well as power lines, transmission lines, and transformer stations; facilities for electricity production from renewable sources; high dams and water reservoirs; facilities for oil and gas production and processing, biofuel production, and biomass facilities.

2) **Transport infrastructure** includes: road, rail, and air transport (highways, state roads of categories I and II; classified and unclassified roads, bridges, tunnels, overpasses, and bus stations; railway networks and stations; airports), inland waterways, ports, and border crossings.

3) **Water management infrastructure** includes: constructed systems for active and passive protection on primary and secondary watercourses; water supply facilities – interregional and regional water supply objects, drinking water treatment plants; flood protection works for urban and rural areas; hydraulic engineering structures on navigable waterways; navigable canals and ship locks not included in the hydroelectric system.

4) **Food supply infrastructure** includes: food production facilities and capacities, food storage facilities (silos, cold storage, etc.), and facilities and means for distribution.

5) **Healthcare critical infrastructure** includes: primary level facilities (health centers, hospitals, pharmacies, institutes); secondary level facilities (general and specialized hospitals); tertiary level facilities (clinics, institutes, clinical-hospital centers, clinical centers), and higher-level healthcare activities (institutes).

6) **Finance** includes: banking, stock exchanges, investment systems, and insurance systems.

7) **Telecommunication and information critical infrastructure** includes: electronic communication system facilities and equipment of international and mainline significance; data transmission systems; information systems; provision of audio and audiovisual media services.

8) **Environmental protection infrastructure** includes: production and storage of hazardous materials (chemical, biological, radiological, nuclear materials, and landfills).

9) **Functioning of government bodies and emergency services** includes: police, emergency medical services, fire and rescue units, and similar services.

10) **Science and education** include: scientific and educational institutions, their facilities, human and material resources.

The **Law on Public-Private Partnerships and Concessions** (Službeni glasnik broj 88/11, 15/16, and 104/16) can be a key factor in protecting critical infrastructure. In today's risk-prone society, where we are exposed to an increasing number of security threats and challenges – ranging from climate change to organized crime and terrorism – cooperation between the private and public sectors is crucial. Regarding collaboration in the field of critical infrastructure protection in Serbia, the private security sector is a very active partner, providing security services. This involves maintaining an adequate level of service quality, including proper equipment, competence, and training, as well as meeting the criteria set by the public procurement system, taking into account the current state of ownership over critical infrastructure (Keković & Ninković, 2020, p. 98).

It is a fact that significant problems arise in the public procurement of private security services, since the sole criterion is the lowest available price (despite the EU directive providing clear guidelines that mandatory criteria should include the economically most advantageous offer and competitive dialogue). The quality of services becomes questionable if the cheapest offer is selected, which can have serious consequences for the protection of critical infrastructure (Keković & Ninković, 2020, p. 98).

Regarding planning documents, critical infrastructure must be treated differently, particularly in preventive activities and emergency response measures, where it must be prioritized. Trends toward improving the protection of critical infrastructure involve a series of procedures, including (Miletić, 2023; Mićović, 2016):

– defining the vision and mission for the development of the critical infrastructure system;

- adopting a strategy;
- focusing on risk assessment;
- developing models for measuring critical infrastructure parameters;
- identifying sources of funding for critical infrastructure;
- educating personnel for critical infrastructure protection;
- establishing an effective public-private partnership model for critical infrastructure protection.

To implement the aforementioned activities, resources are essential. The basic resources include human, material, spatial, temporal, and knowledge and information resources. These resources have a decisive impact on the effectiveness of responses to challenges, risks, and threats to the safety of people, material assets, and the environment, and thus on protection against all types of risks in any form of emergency. It is necessary to ensure the continuity of resource management in all phases of emergency management (Jakovljević, 2010).

An effective critical infrastructure management system requires establishing an organizational structure, dividing responsibilities, developing procedures, and ensuring proper resource allocation. Organizations should define guidelines for developing an emergency management model based on their current state and environmental requirements to enable an adequate response to potential risks and threats (Jakovljević, 2010).

Regarding the protection of critical infrastructure, the European Union plays a significant role. It has launched numerous initiatives and a range of research programs to study various aspects of threats to critical infrastructure. The Republic of Serbia, which is a candidate for EU accession, must implement and apply specific requirements. European Commission Directive 2008/114/EC serves as the basis for subsequent steps in defining criteria for critical infrastructure. Annex III of the same document outlines procedures that each member state must implement through several steps (Mićović, 2016):

Step 1 – Each Member State applies sectoral criteria to make an initial selection of critical infrastructure within the sector.

Step 2 – Each Member State applies the definition of critical infrastructure under Article 2(a) to the potential European Critical Infrastructure (ECI) identified in Step 1.

Step 3 – Each Member State applies the cross-border element of the ECI definition under Article 2(b) to the potential ECI that has passed the first two steps of this procedure. A potential ECI that meets the definition will proceed to the next step of the procedure. For infrastructure providing an essential service, the availability of alternatives and the duration of disruption/recovery will be taken into account.

Step 4 – Each Member State applies cross-cutting criteria to the remaining potential ECIs. Cross-cutting criteria consider: the severity of the impact; the availability of alternatives for infrastructure providing an essential service; and the duration of disruption/recovery. Potential ECIs that do not meet the cross-cutting criteria will not be considered ECIs.

This directive represented the first step in identifying European critical infrastructure and emphasized the need for enhanced protection. It also highlighted the focus on the transport and energy sectors, but it should also be considered in terms of assessing inter-sectoral impacts, especially in the information and communication technology sector (Mićović, 2016; Škero & Ateljević, 2015).

6. Conclusion

To achieve sustainable development, the primary task is to reduce vulnerability and increase the resilience of critical infrastructure. Understanding the importance of critical infrastructure for human and national security is a prerequisite for adopting and implementing adequate protection strategies, which ensure an acceptable level of losses and damage in the face of natural hazards, as well as external and internal threats (Cvetković, 2020; Cvetković & Martinović, 2020; Cvetković, 2022).

In the face of various crisis events that negatively affect the economy, ecosystems, economic development, and society as a whole, the development and strengthening of the concept of critical infrastructure protection

is of fundamental importance. This concept involves understanding the nature of risks and developing preparedness to prevent or mitigate negative consequences. Continuous adaptation to emerging risks and threats enables the acquisition of broader competencies to respond effectively to crisis events (Košanin, 2018; Sarriegi & Hernantes, 2013).

The population depends on certain services provided within the local community, and its vulnerability often varies with the nature of those services. For example, instead of relying on a single extensive water supply system, it is desirable to have a network of smaller, independent water supply facilities. In the event of floods, it is unlikely that all water supply facilities would be destroyed or damaged. In such cases, the unaffected facilities would continue to provide essential water supply to residents in the flood-affected areas (Cvetković, 2020, p. 519; Parker et al., 1997).

The primary step in defining and protecting critical infrastructure is recognizing its significance in the Republic of Serbia's highest strategic documents (Mladenović & Komazec, 2022). The existing challenges and problems in Serbia regarding critical infrastructure protection cannot be resolved solely by adopting the Law on Critical Infrastructure, but also require the adoption of other documents and subordinate acts with all necessary amendments and harmonizations of the legal framework. Another key factor is the political will to implement strategic goals, as well as adequate education for the owners and operators of critical infrastructure.

Measures and procedures are the responsibility of owners, operators, or users and must be continuously prepared and implemented. Concrete, practical recommendations for policymakers and critical infrastructure operators include:

- First, identifying the risks, threats, and vulnerabilities to which specific systems are exposed;
- Creating critical infrastructure maps;
- Enabling adequate information exchange;
- Training employees engaged in critical infrastructure protection systems;
- Developing recovery plans in the event of an emergency;
- Investing in outdated infrastructure facilities.

The complexity of risks and threats, and the fact that their occurrence endangers the capacities of critical infrastructure and its regular functioning, indicate the need to undertake and develop actions aimed at (Škero & Ateljević, 2015):

1. Understanding the elements of criticality and vulnerability of different state infrastructures;
2. Defining measures to reduce vulnerabilities;
3. Developing contingency plans for emergencies;
4. Promoting awareness among public and private operators regarding critical infrastructure protection measures;
5. Developing international cooperation.

7. References

1. Aktar, M. A., Shohani, K., Hasan, M. N., & Hasan, M. K. (2021). Flood vulnerability assessment by flood vulnerability index (FVI) method: a study on Sirajganj Sadar Upazila. *International Journal of Disaster Risk Management*, 3(1), 1-14.
2. Barney, D. (2019). Beyond carbon democracy: Energy, infrastructure, and sabotage. Energy culture: Art and theory on oil and beyond, 214-228.
3. Biringer E. B., Vugrin D. E., Warren E. D.: Critical Infrastructure System Security and Resiliency, Taylor & Francis Group, 2013.
4. Cvetković, V. & Mijalković, S. (2013). Spatial and Temporal Distribution of Geophysical Disasters. Serbian Academy of Sciences and Arts and Geographical Institute Jovan Cvijic, Journal of the Geographical In-

stitute "Jovan Cvijić" 63/3, 345-360, SASA: Special issue: *International Conference Natural Hazards Links Between Science and Practice.*

5. Cvetković, V. (2013). *Interventno-spasilačke službe u vanrednim situacijama.* Beograd. Zadužbina Andrejević
6. Cvetković, V. (2014). Zaštita kritične infrastrukture od posledica prirodnih katastrofa. *In Sedma međunarodna znastveno-stručna konferencija,, Dani kriznog upravljanja;. Hrvatska: Velika Gorica* (Vol. 22, pp. 1281-1295).
7. Cvetković, V. (2020). *Upravljanje rizicima u vanrednim situacijama*. Beograd. Naučno-stručno društvo za upravljanje rizicima u vanrednim situacijama.
8. Cvetković, V. (2022). *Taktika zaštite i spasavanja u katastrofama.* Beograd. Naučno-stručno društvo za upravljanje rizicima u vanrednim situacijama.
9. Cvetković, V. (2023). *Otpornost na katastrofe: vodič za prevenciju, reagovanje i oporavak.* Beograd. Naučno-stručno društvo zaupravljanje rizicima u vanrednim situacijama.
10. Cvetković, V., & Stojković, D. (2015). Knowledge and perceptions of secondary school students in Kraljevo on natural disasters.*Ecologica*, 22(77), 42-48.
11. Cvetkovic, V., & Martinović, J. (2020). Innovative solutions for flood risk management. *International Journal of Disaster Risk Management,* 2(2), 71-100.
12. Cvetković, V., & Planić, J. (2022). Earthquake risk perception inBelgrade: implications for disaster risk management. *International Journal of Disaster Risk Management*, 4(1), 69-88.
13. Cvetković, V., Flipović, M. (2017). *Pripremljenost za reagovanjena rizike od prirodnih katastrofa.* Zadužbina Andrejević.
14. Cvetković, V., Milojković, B., Stojković, D. (2014). Analiza geoprostorne i vremenske distribucije zemljotresa kao prirodnih katatrofa. *Vojno delo*, 66(2), 166-185.
15. Degg, M. (1992). Natural disasters: recent trends and prospects. *Geography*, 77(3), 198-209.
16. ISDR, UN. (2009). UNISDR terminology on disaster risk reduction. Geneva.
17. Jakovljević, V. (2010). Resursi kritične infrastrukture i njihov značaj za upravljanje vanrednim situacijama. *Godišnjak Fakulteta bzebednosti*, 63-81.
18. Jakovljević, V., & Gačić, J. (2012). Zaštita kritične infrastrukture u kriznim situacijama. *In Zbornik radova= Proceedings/Međunarodna naučna konferencija Menadžment 2012, Mladenovac, 20-11. april 2012= International Scientific Conference Management 2012. Mladenovac: Fakultet za industrijski menadžment, ICIM plus-Izdavački centar za industrijski menadžment plus*.
19. Janković, L., Cvetković, V. M., Gačić, J., Renner, R., & Jakovljević, V. (2025). Integrating Psychosocial Support into Emergency and Disaster Management, and Public Safety: The Role of the Red Cross of Serbia.
20. John, D. K. S., Mohammed, H. A., Diana, M., & Ajayi, E. O. (2025). Security of Information Resources in Federal College of Education Libraries in Northwest Nigeria. *International Journal of Contemporary Security Studies*, 1(1), 85-98.
21. Karabacak, B., & Tatar, Ü. (2014). Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection. *Critical Infrastructure Protection,* 116, 63.
22. Kaur, B. (2020). Disasters and exemplified vulnerabilities in a cramped Public Health Infrastructure in India. *International Journal of Disaster Risk Management,* 2(1), 15-22.
23. Komazec, N. (2023). Kritična infrastruktura u kontekstu održivog razvoja: izazovi i perspektive. *Zbornik radova naučno-stručne konferencije*, 21.
24. Korajlić, N., & Marjanović, M. (2022). Uticaj prirodnih katastrofa na funkcionisanje kritične infrastrukture. *Zbornik radova naučno-stručne konferencije*, 181.
25. Košanin, V. (2018). Kritična transportna infrastruktura i krizni menadžment. *Zbornik radova Fakulteta tehničkih nauka u Novom Sadu.*

26. Krstić, M. (2016). Izazov definisanja savremenog terorizma. U: *Vojno delo* 3/2016. Beograd.
27. Kumiko, F. & Shaw, R. (2019). Preparing an international joint project: Use of Japanese flood hazard map in Bangladesh. *International Journal of Disaster Risk Management*, 1(1), 62-80
28. Lewis, T. (2006). Infrastructure Protection in Homeland Security, Defending a Networked Nation, Wiley Interscience.
29. Lukas, L., & Hromada, M. (2011). Resilience as main part of protection of critical infrastructure. *International journal of mathematical models and methods in applied sciences*, 5(6), 1135–1142.
30. Mančić, T. (2025). Climate Change as a Security Challenge, Risk and Threat of the 21st Century and Its Consequences on Critical Infrastructure. *International Journal of Contemporary Security Studies,* 1(1), 191-204.
31. Metodologija izrade i sadržaj procene rizika od katastrofa i plana zaštite i spasavanja, *Službeni glasnik broj* 80/2019.
32. Mićović, M. D. (2016). *Bezbednosni aspekti funkcionisanja kritične infrastrukture u vanrednim situacijama* (Doktorska disertacija, Univerzitet u Beogradu-Fakultet bezbednosti).
33. Mićović, M. D. (2020). *Specifičnosti kritične infrastrukture u Republici Srbiji.* Beograd. Kriminalističko-policijski univerzitet.
34. Milenkovic, D. (2025). Theoretical, Institutional and Organizational Aspects of the Integrated Disaster Risk Reduction System: Towards a Deeper Understanding of Disaster Resilience in Serbia. *International Journal of Contemporary Security Studies*, 1(1), 175-190.
35. Miletić, S. (2023). *Značaj funkcionisanja i zaštite kritične infrastrukture u vanrednim situacjama*. Master rad. Univerzitet u Beogradu Fakultet bezbednosti.
36. Mladenović, M., & Komazec, N. (2022). Normativni okvir kritične infrastrukture u Republici Srbiji. *Zbornik radova*: Naučno-stručne konferencije „Diskurs o kritičnoj infrastrukturi".
37. Ninković, V. M. (2024). *Otpornost kritične infrastrukture na nerutinske rizike* (Doctoral dissertation, University of Belgrade (Serbia).
38. Ocal, A. (2019). Natural Disasters in Turkey: Social and Economic Perspective. *International Journal of Disaster Risk Management,* 1(1), 51-61.
39. Onuma, H., Shin, K. J., & Managi, S. (2017). Household prepa-redness for natural disasters: Impact of disaster experience andimplications for future disaster risks in Japan. *International journal of disaster risk reduction,* 21, 148-158.
40. Parker, D., Islam, N., & Weng Chan, N. (1997). Reducing vulnerability flolowing flood disadters: issues and practices. In Reconstruction after disaster: Issues and practices (pp. 23-24). Ashgate Publishing.
41. Perić, J., & Cvetković, V. (2019). Demographic, socio-economic and phycological perspective of risk perception from disasters caused by floods: case study Belgrade. *International Journal of Disaster Risk Management*, 1(2), 31-43.
42. Pribičević, N., Janković, K., Živković, M. (2022). Prevencija rizika od terorizma kao savremenog obilika ugrožavanja kritične infrastrukture. *In naučno-stručna konferencija* 8p.157.
43. Ptáček, B., & Skoruša, L.(2015). Cyber criminality.
44. Rakić, M. M. (2015). *Krizni menadžment u funkciji zaštite kritičnih infrastruktura u zemljama u tranziciji*. Univerzitet u Beogradu.
45. Sarriegi, M., & Hernantes, J. (2013). *Resilience Framework for Critical Infrastructures*, Universidad de Navarra, Donostia, San Sebastian.
46. Shaikh, S. A., Chivers, H., Nobles, P., Clark, J. A., & Chen, H. (2008). Network reconnaissance. *Network Security,* 2008(11), 12-16.
47. Stajić, Lj. (2015). *Osnovi sistema bezbednosti – sa osnovama istraživanja bezbednosnih pojava.* Novi Sad: Pravni fakultet.

48. Strategija nacionalne bezbednosti Republike Srbije, *Službeni glasnik broj* 94/2019.

49. Strategija odbrane Republike Srbije, *Službeni glasnik broj* 94/2019.

50. Trbojević, M. (2018). *Zaštita kritičnih infrastruktura - iskustva tranzicionih zemalja*. Beograd: Institut za političke studije.

51. Uredba o kriterijumima za identifikaciju kritične infrastrukture i načinu izveštavanja o kritičnoj infrastrukturi Republike Srbije, *Službeni glasnik broj* 69/2022.

52. Vidović, N., & Beriša, H. (2025). Economic Aspects of Cyber Security: Socio-Financial Consequences of Cyber Attacks. *International Journal of Contemporary Security Studies*, 1(1), 149-162.

53. Vlada Republike Srbije. (2014). *Izveštaj o elementarnoj nepogodi – poplavi koja je zadesila Republiku Srbije i merama koje su preduzete radi spsavanja stanovništva i odbrane ugroženih mesta od poplava.* Retrieved from http://www.parlament.gov.rs/upload/archive/files/cir/pdf/akta_procedura /2014/2220-14.pdf

54. Vračević, N. (2025). Strategic Roles of Private Military Companies: The Evolution and Privatization of Warfare in the Context of Contemporary Global Conflicts. *International Journal of Contemporary Security Studies*, 1(1), 163-174.

55. Zakon o javno-privatnom partnerstvu i koncesijama, *Službeni glasnik broj* 88/11, 15/16 i 104/16.

56. Zakon o kritičnoj infrastrukturi, *Službeni glasnik broj* 87/2018.

57. Zakon o smanjenu rizika od katastrofa i upravljanju u vanrednim situacijama, *Službeni glasnik broj* 87/2018.

58. Zubrzycki, W. (2017). The Security of the Republic of Poland's Maritime Areas and the Polish Coast in the Context of Terrorist Attacks. *Internal Security*, 9, 169-187.

59. Škero, M., & Ateljević, V. (2015). "Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa Direktivom Saveta Evrope 2008/114/ES." *Vojno delo* 67.3, 192-207.