

Article

Not peer-reviewed version

---

# Optimising Disaster Resilience Through Advanced Risk Management and Financial Analysis of Critical Infrastructure in the Serbian Defence Industry

---

Nikola Vidović , Hatidža Beriša , [Vladimir M. Cvetković](#) \*

Posted Date: 16 July 2024

doi: 10.20944/preprints202407.1228.v1

Keywords: disaster risk management; resilience; risk management; financial analysis; critical infrastructure; security; defence; Serbia



Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

## Article

# Optimising Disaster Resilience through Advanced Risk Management and Financial Analysis of Critical Infrastructure in the Serbian Defence Industry

Nikola Vidović<sup>1</sup>, Hatidža Beriša<sup>1,2</sup>, Vladimir M. Cvetković<sup>2,3,4,\*</sup>

<sup>1</sup> University of Defence, Military Academy – Belgrade, Republic of Serbia; vidovicnikola.finance@gmail.com (N.V.); berisa.hatidza@gmail.com (H.B.)

<sup>2</sup> Department of Disaster Management and Environmental Security Studies, Faculty of Security Studies, University of Belgrade, Gospodara Vucica 50, 11040 Belgrade, Serbia

<sup>3</sup> Scientific-Professional Society for Disaster Risk Management, Dimitrija Tucovića 121, 11040 Belgrade, Serbia

<sup>4</sup> International Institute for Disaster Research, Dimitrija Tucovića 121, 11040 Belgrade, Serbia

\* Correspondence: vmc@fb.bg.ac.rs

**Abstract:** This paper presents a comprehensive analysis of the financial factors and risk management strategies essential for optimizing disaster resilience within the Serbian defence industry's critical infrastructure. The significance of this sector is multi-faceted, impacting national security, economic stability, and technological advancement. Primarily, the Serbian defence industry ensures the preservation of vital defence interests, maintaining Serbia's independence from foreign sources for weapons and military equipment in both peacetime and wartime. Economically, it is a significant employer of the working-age population, directly affecting local employment rates, fostering economic development, and ensuring the sustainable growth of this crucial sector. This, in turn, stimulates broader economic activity and enhances social cohesion while strengthening the national balance of payments through increased export potential. From a technological perspective, the defence industry drives scientific, technological, and industrial development, reinforcing Serbia's global political and military standing within the Western Balkans and on the international stage. Consequently, the paper aims to examine the risk management and protection of the Serbian defence industry's critical infrastructure, offering concrete and actionable measures to improve and develop these systems with a particular emphasis on security. The research's utility and contribution lie in identifying similarities and differences in the operational performance of defence industry companies, a vital segment of the national economy. The presentation of these findings focuses on the protection of critical infrastructure. The results will form the basis for further investigation into the underlying causes of business performance and the effective management of critical infrastructure security.

**Keywords:** disaster risk management; resilience; risk management; financial analysis; critical infrastructure; security; defence; Serbia

## 1. Introduction

National security, as well as overall security, heavily depends on the robustness of critical infrastructure. Initially viewed as a logistical function that supports other logistical operations, critical infrastructure has gained prominence due to the rising threat of asymmetric attacks, particularly terrorism. Both theoretical analyses and practical experiences have shown that critical infrastructure systems, services, and assets—whether physical or virtual—are crucial for societal well-being. The disruption or destruction of these systems can severely impact citizens' health, safety, economic stability, and the effective functioning of government (Škero & Ateljević, 2015).

Critical infrastructure comprises large-scale, man-made systems that are crucial for the production and distribution of essential goods and services. These systems include but are not limited to, the provision of energy, water, data, transportation, finance, and healthcare. According to the Council Directive 2008/114/EC, an infrastructure is deemed critical if its incapacitation or destruction would have a significant impact on public health, safety, security, economic stability, and social well-being. The failure or disruption of critical infrastructure can lead to severe societal and economic repercussions, potentially causing cascading failures across other interconnected infrastructures, and resulting in catastrophic consequences (Carreras et al., 2004; Zio, 2016).

Recent research underscores the growing interconnectedness of critical infrastructure systems, which heightens their susceptibility to both natural and human-made hazards. For instance, the rising integration of information and communication technologies has introduced new cyber risks that could jeopardize physical infrastructure (Petit et al., 2015). Additionally, climate change has brought about new challenges, such as extreme weather events, that can disrupt essential services and demand stronger resilience planning (Rinaldi et al., 2001). Hence, a thorough approach to risk management is crucial to safeguarding these essential systems and maintaining their operation amid various threats.

Regarding that, the objective of this paper is to systematically examine the vulnerabilities and risk factors associated with the critical infrastructure of the Serbian defence industry through a financial performance analysis. This study reflects on the inherent complexities of these systems, identifies related challenges, and proposes potential solutions for their analysis and management. Specifically, the paper explores the framework of vulnerability and risk analysis in protecting and enhancing the resilience of six key entities within Serbia's defence industry. Given the complexity of these systems, the study argues for the integration of various modelling perspectives and innovative analytical approaches (Bouchon, 2006). This integration is crucial for accurately capturing the structural and dynamic complexities of critical infrastructures, thereby enabling confident decision-making regarding protection and resilience actions (Zio, 2016).

## **2. Critical Infrastructure Resilience: A Risk and Vulnerability Approach**

The Republic of Serbia has a wealth of experience in handling disasters, particularly those stemming from electrical incidents. In the last ten years, the country has recorded over 150,000 fires (Cvetković, Pavlović, & Janković, 2021; Cvetković, Pavlović, & Janković, 2021; Cvetković et al., 2022; Cvetković & Marković, 2021; Cvetković & Janković, 2021). Significant incidents, such as the 2014 floods in Obrenovac and the 2009 earthquakes in Kraljevo, have driven Serbia to establish a comprehensive protection and rescue system to effectively address threats to critical national resources (Cvetković, Babić, & Gačić, 2017; Cvetković, Bošković, & Ocal, 2021; Cvetković & Martinović, 2020; Cvetković, 2016). The legislative framework, including the Law on Emergency Situations and various strategic documents, lays the groundwork for adopting the Critical Infrastructure Law and aligns with numerous European regulations in this area (Cvetković & Synodinou, 2024; Cvetković, Nikolić, & Lukić, 2024; Cvetković, Nikolić, & Lukić, 2024; Cvetković & Šišović, 2023; Cvetković & Šišović, 2024; Cvetković et al., 2021).

Serbia's defence industry's critical infrastructure faces numerous hazards, risks, and threats, including natural disasters, ageing components, increased load demands, climate change, intentional attacks, and terrorism. As a result, protecting critical infrastructure (CIP) has become a major global priority. Regional countries like Slovenia and Croatia are actively addressing these issues through specific legislation that outlines institutional roles during disasters (Lewis, 2006), with a focus on physical protection and asset reinforcement (Cimellaro et al., 2010). To protect the defence industry's critical infrastructure, it is crucial to model its components under various threats and perform thorough risk and vulnerability assessments at the system level.

The importance of resilience in critical infrastructure—its ability to endure, adapt, and quickly recover from disruptions—has been highlighted by recent catastrophic disasters (Moteff, 2012). The 2005 World Conference on Disaster Reduction emphasized the need for disaster resilience, fostering a new culture of disaster response (Zio, 2016). Systems must be not only reliable but also capable of

recovering from disruptions. Government policies now encourage efforts to ensure systems can continue operating at some level or return to full functionality after a disruption (Cvetković, Rikanović, & Knežević; Cvetković & Šišović, 2024; Grozdanić & Cvetković, 2024). Consequently, resilience is now seen as an essential attribute for critical infrastructure, integrated into its design, operation, and management. Serbia should play a significant role in further defining and regulating this area.

The national well-being of Serbia's defence industry, along with all interconnected entities and stakeholders, relies on secure and resilient critical infrastructure—resources, systems, and networks crucial for the seamless functioning of society. To achieve security and resilience, critical infrastructure partners must collaboratively prioritize goals, mitigate risks, measure progress, and adapt to changing conditions (U.S. DHS, 2013). Although Serbia has recently established and prioritized critical infrastructure compared to the European Union, the United States, and neighbouring countries, substantial efforts by the academic, professional, and scientific communities, along with institutional support, guide national efforts toward critical infrastructure risk management.

The community involved in critical infrastructure risk management is diverse, including partnerships between owners and operators, government entities at various levels, regional organizations, non-profit groups, and academia. Effective risk management requires an integrated approach across this community (Carla, 2019; Cvetković, 2019; Goyal, 2019; Mano & Rapaport, 2019; Öcal, 2019; Vibhas, Bismark, Ruiyi, Anwaar, & Rajib, 2019; Xuesong & Kapucu, 2019): a) identify, deter, detect, disrupt, and prepare for threats against the state's critical infrastructure, including the defence system, the Ministry of Defence, the Armed Forces of Serbia, and the defence industry; b) reduce the vulnerability of critical assets, systems, and networks within the defence industry and its external relations; c) mitigate the potential impacts of incidents or adverse events on critical infrastructure. The success of this integrated approach depends on leveraging a broad spectrum of skills, expertise, and experience within the critical infrastructure community and related stakeholders. This has become increasingly evident in Serbia in recent years. Effective information sharing among partners is crucial for building situational awareness and enabling risk-based decision-making (U.S. DHS, 2013).

Traditionally, risk has been defined as a function of three elements: the threats to which an asset is susceptible, the asset's vulnerabilities to the threat, and the potential consequences of asset degradation (Petit et al., 2013). Today, resilience has emerged as a fourth component, alongside vulnerability, threat/hazard, and consequences, forming the comprehensive risk function. In the context of critical infrastructure, risk at an asset (such as an office building, hangar, factory, or machinery) for a given threat/hazard type is a function of the threat/hazard likelihood (Carlson et al., 2012), the asset's vulnerability (the likelihood of a successful threat event), the asset's resilience, and the magnitude of the resulting consequences (Petit et al., 2013). As depicted in Figure 1, the risk components are inherently interdependent. When considering a threat or hazard—whether manmade or natural—the vulnerability and resilience of the asset (infrastructure) will determine the resultant consequences. The intrinsic complexity of risk is amplified by dependencies and interdependencies that affect the components of risk (Petit et al., 2015). In today's interconnected world, the potential impacts are exacerbated by these dependencies and the diverse range of threats capable of exploiting them. Critical infrastructure now spans national borders and global supply chains, a crucial point in this case study.

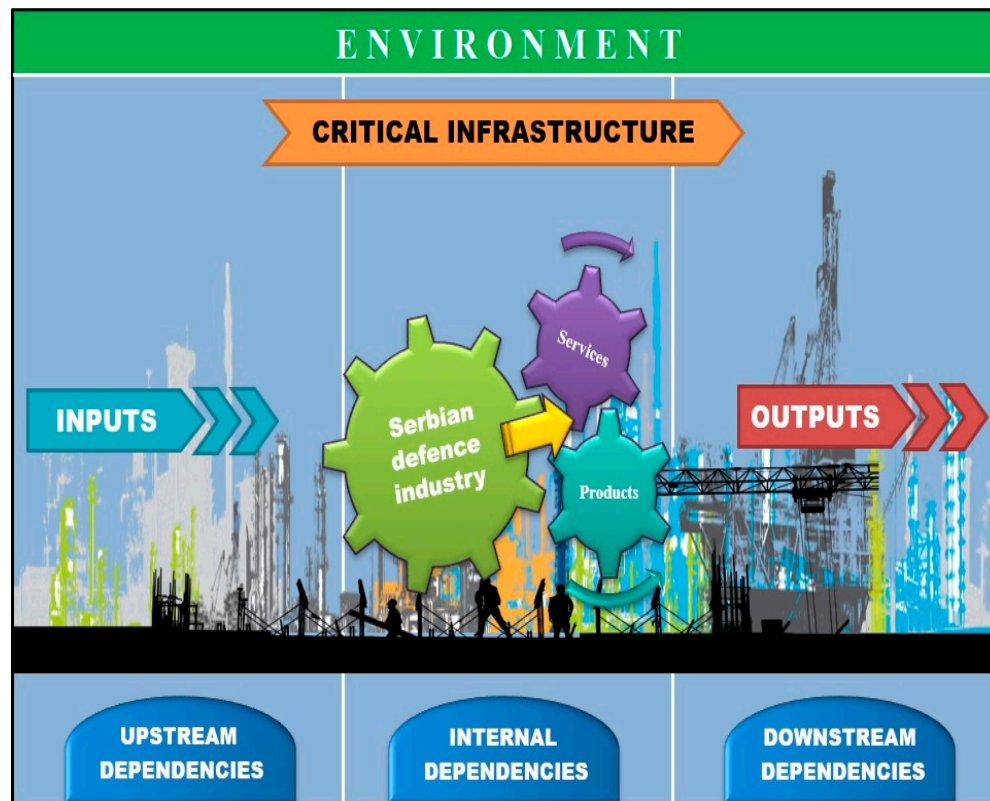


**Figure 1.** The interdependence of risk components: a comprehensive analysis of their interconnected nature and implications for effective risk management.

Within the context of the risk framework depicted, policy, and operating environments, the structures of critical infrastructure sectors and cross-sector partnerships provide a framework to guide the collective efforts of partners. The national effort to enhance critical infrastructure security and resilience relies on the ability of public and private critical infrastructure owners and operators to make risk-informed decisions when allocating limited resources during both steady-state and crisis operations (U.S. DHS, 2013). The complex and uncertain risk environment affecting critical infrastructure, particularly the defence industry, has evolved significantly over the past decade. Daily threats to vital state entities have become increasingly relevant, as evidenced by developments globally, regionally, and in Serbia's southern province. For example, critical infrastructure that has long faced physical threats and natural disasters is now increasingly exposed to cyber risks, stemming from the integration of information and communication technologies with critical infrastructure operations and the hostile exploitation of potential cyber vulnerabilities.

As the number of threats in modern analyses and practice continues to grow, protecting critical infrastructure becomes increasingly important (Carla S., 2019; Cvetković, 2019; Frostdick, 1997; Kumiko & Shaw, 2019; Öcal, 2019; Perić & Cvetković, 2019; Vibhas et al., 2019). This protection is crucial not only because of the potential damage to the infrastructure itself but also because of the broader societal and economic consequences such damage can cause. Protecting critical infrastructure during emergencies should be viewed as part of a comprehensive prevention process and emergency response strategy. In this context, organizations establish, implement, and maintain procedures to identify potential incidents that could negatively impact them, their activities, and the environment (Cvetković, 2024b). These procedures aim to protect lives and property, prevent emergencies or disasters, minimize operational downtime, recover critical activities, return to normal operations, and safeguard the organization's reputation. As Rinaldi, Peerenboom, and Kelly note, "It is impossible to adequately analyze or understand the behaviour of a given infrastructure [organization] in isolation from the environment or other infrastructures" (Rinaldi, Peerenboom, and Kelly, 2001). Critical infrastructure constantly interacts with its environment, utilizing and transforming inputs from the environment to provide outputs back to it. Figure 1 illustrates how the critical infrastructure of Serbia's defence industry influences and interacts with its environment.





**Figure 2.** Influence and interaction between critical infrastructure of Serbian defence industry and environment.

These interactions can be classified into three main categories: a) upstream dependencies: which refer to the essential products or services provided to one infrastructure by another external infrastructure. In the context of the Serbian defence industry, there is a direct dependency on companies and entities that supply vital raw materials, supplies, and resources for the production of weapons and military equipment. Additionally, these external entities offer services that the defence industry cannot provide independently.

Protecting these upstream dependencies from various risks and threats across all operational domains is crucial; b) internal dependencies: involve the interactions among the internal operations, functions, and missions within the infrastructure itself. Internal dependencies are the internal connections among the assets that make up critical infrastructure. For example, the production of ammunition at “Prvi Partizan” a.d. Užice is directly reliant on the propulsion machinery and the moulds that determine the calibre; c) downstream dependencies: These pertain to the effects on a critical infrastructure’s consumers or recipients resulting from the degradation of the resources provided by that infrastructure. In a more specific sense, the Ministry of Defence and all units of the Serbian Armed Forces would be directly impacted. In a broader sense, the entire state, the population, the environment, and the functioning of interstate entities and organizations would also be affected.

### 3. Improving National Efforts for Strengthening the Security of Critical Infrastructure

The government, particularly through the Ministry of Defence and the defence industry sector, has a vested interest in ensuring the robustness of critical infrastructure and the continuous provision of essential services under all conditions. Owners and operators of critical infrastructure often stand to gain the most from investing in their security and resilience. They are motivated by both the direct benefits and a sense of social responsibility to adopt these practices. However, production sectors

and companies may be rightfully concerned about the return on investments in security and resilience, as these may not yield immediately measurable benefits. Effective incentives can help justify the costs associated with enhanced security and resilience by balancing short-term expenses with near-term benefits (U.S. DHS, 2013).

Market-based incentives can drive significant changes in business practices and foster the development of markets such as insurance for cyber, chemical, biological, or radiological risks. Additionally, the Republic of Serbia and local governments can explore offering incentives to encourage investment in security and resilience measures. Effective measures and activities for implementation include: a) continuously identifying, analyzing, and, where appropriate, implementing incentives; b) supporting research and data collection to quantify the potential costs resulting from inadequate critical infrastructure security and resilience, and insufficient cyber preparedness; c) establishing innovation challenge programs to incentivize new solutions for strengthening infrastructure security and resilience during the planning, design, and redesign phases, including technological, engineering, and process improvements.

The dependencies and interdependencies of critical infrastructure represent complex elements that are challenging to identify and analyze. They are characterized by various interactions (e.g., upstream, internal, and downstream), classes (e.g., physical, cyber, logical, and geofunctional), and dimensions (e.g., operating environment, coupling and response behaviour, type of failure, infrastructure characteristics, and state of operation). These factors influence all components of risk (threat/hazard, vulnerability, resilience, and consequence), can themselves become threats or hazards, affect the resilience and protection performance of critical infrastructure, and lead to cascading and escalating failures. It is essential to integrate dependencies and interdependencies into risk and resilience methodologies.

A data-driven capability that operationalizes the analysis of dependencies and interdependencies would not only provide an unprecedented level of situational awareness but also enable decision-makers to anticipate disruptions. Achieving this ultimate goal requires the development of a comprehensive and interactive assessment of critical infrastructure dependencies and interdependencies. This necessitates the combination of multiple areas of expertise (e.g., engineering, social sciences, business continuity, and emergency management) within an adaptive and flexible assessment framework (Petit et al., 2015).

Furthermore, the integration of advanced technologies and innovative methodologies plays a crucial role in enhancing the security and resilience of critical infrastructure (Vladimir Cvetković, 2024a, 2024b). Emerging technologies such as artificial intelligence, machine learning, and big data analytics can be leveraged to predict and mitigate potential risks more effectively (V. Cvetković & Filipović, 2017). By utilizing these technologies, critical infrastructure systems can benefit from real-time monitoring, predictive maintenance, and automated response mechanisms that can significantly reduce vulnerabilities and enhance overall resilience. Additionally, collaboration with international partners and participation in global initiatives can provide valuable insights and best practices, fostering a more comprehensive approach to critical infrastructure protection (Baruh, Dey, & Dutta, 2023; V. M. Cvetković, 2023; El-Mougher, Abu Sharekh, Abu Ali, & Zuhud, 2023; Rajani, Tuhin, & Rina, 2023; Sudar, Cvetković, & Ivanov, 2024). The Republic of Serbia, by embracing these advancements and fostering a culture of continuous improvement, can strengthen its national efforts to secure and sustain its critical infrastructure, ultimately contributing to the stability and prosperity of the nation (Cvetković & Kezunović, 2021; Hromada & Lukas, 2012; Murray & Grubescic, 2012).

#### **4. Comprehensive Financial Analysis of Entities in the Defence Industry**

The Defence Industrial Base Sector in Serbia is the national industrial complex responsible for research and development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts. This complex aims to meet the military requirements of the Serbian Armed Forces, third countries, and developing nations, as well as some of the most powerful armies worldwide, including the U.S. military and security sectors (Table 1). The defence industry in Serbia comprises numerous companies engaged in the production and trade of weapons,

military equipment, and dual-purpose goods (items usable for both military and civilian purposes). These companies are both state-owned and privately owned (Radić & Radić, 2018). The Ministry of Defence of the Republic of Serbia has significant authority over the majority of state-owned companies, managing and supervising their operations following the Law on Defence.

**Table 1.** Comparative Financial Analysis of Serbian Defence Industry Companies (2014-2017). Source: Authors’ calculation based on financial reports.

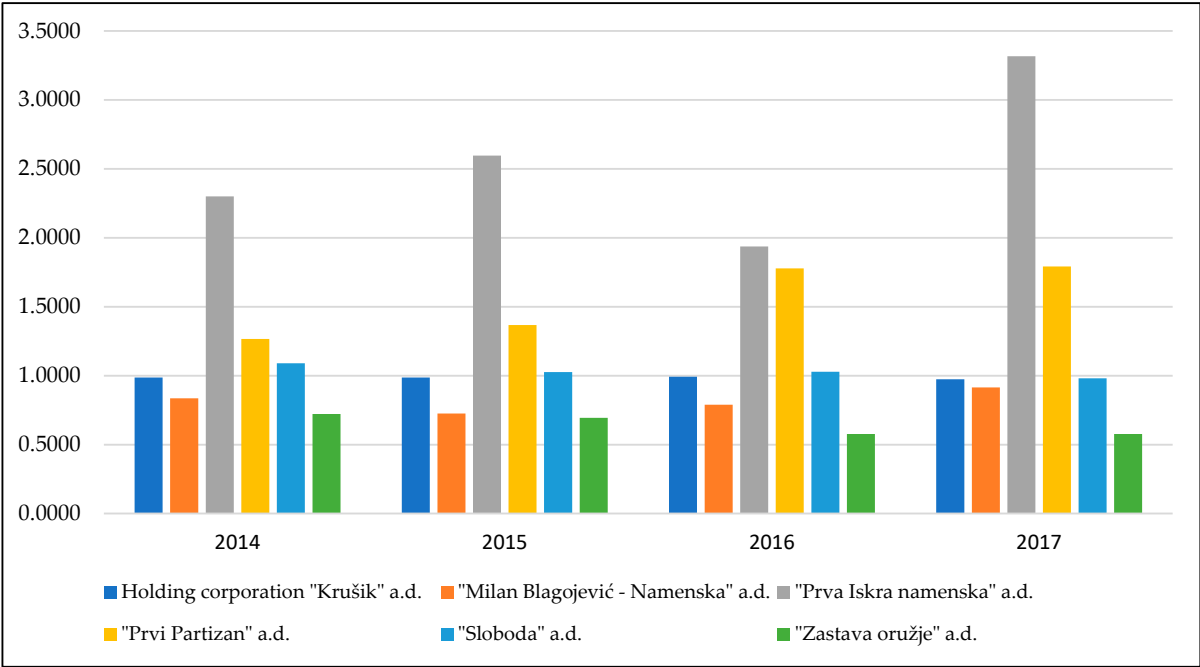
No.		1	2	3	4	5	6
Company of Serbian defence industry		Holding corporation "Krušik" a.d.	"Milan Blagojević - Namenska" a.d.	"Prva Iskra namenska" a.d.	"Prvi Partizan" a.d.	"Sloboda" a.d.	"Zastava oružje" a.d.
City		Valjevo	Lučani	Barič	Užice	Čačak	Kragujevac
INDICATOR		RATIO OF CURRENT LIQUIDITY					
Business year	2014	0.9871	0.8361	2.3003	1.2667	1.0889	0.7228
	2015	0.9862	0.7259	2.5965	1.3680	1.0259	0.6938
	2016	0.9919	0.7895	1.9366	1.7782	1.0279	0.5769
	2017	0.9739	0.9151	3.3162	1.7924	0.9813	0.5768
INDICATOR		BUSINESS PROFIT RATIO					
Business year	2014	-0.0181	0.1490	-0.0972	0.0801	0.1565	-0.0407
	2015	0.1400	0.1376	-0.0481	0.1702	0.0249	0.0675
	2016	0.0971	0.1745	0.1650	0.1666	0.1607	-0.0335
	2017	0.1184	0.2340	0.1476	0.0424	0.1052	-0.0128
INDICATOR		TURNOVER RATIO OF TOTAL ASSETS					
Business year	2014	0.3277	0.4795	0.2602	0.6015	0.4398	0.2725
	2015	0.4735	0.5670	0.2927	0.7162	0.3823	0.2800
	2016	0.4701	0.7196	0.6947	0.6820	0.5034	0.2298
	2017	0.7534	0.6927	0.7222	0.4068	0.5752	0.1989
INDICATOR		DEBT RATIO					
Business year	2014	0.2896	0.4783	0.6173	0.5436	0.4355	0.2538
	2015	0.2760	0.4678	0.6622	0.5986	0.4229	0.1961
	2016	0.2107	0.5002	0.7271	0.6894	0.3787	0.1262
	2017	0.1820	0.5238	0.6804	0.4619	0.3659	0.0863
INDICATOR		LEVERAGE					
Business year	2014	3.4529	2.0907	1.6200	1.8396	2.2962	3.9401
	2015	3.6232	2.1375	1.5102	1.6704	2.3647	5.1001
	2016	4.7472	1.9993	1.3754	1.4506	2.6407	7.9249
	2017	5.4934	1.9093	1.4697	2.1648	2.7333	11.5905
INDICATOR		ROE (Return on Equity)					
Business year	2014	-0.1617	0.0087	0.0136	0.1241	0.0073	-0.4573
	2015	0.1076	0.0146	0.0076	0.2189	0.0149	-0.0617
	2016	0.2056	0.1372	0.0354	0.1604	0.1143	-0.3887
	2017	0.3482	0.2418	0.1046	0.0701	0.0850	-0.3132
INDICATOR		ROA (Return on Assets)					



<div>Business</div> <div>year</div>	2014	-0.0059	0.0714	-0.0253	0.0482	0.0688	-0.0111
	2015	0.0663	0.0780	-0.0141	0.1219	0.0095	0.0189
	2016	0.0456	0.1256	0.1146	0.1137	0.0809	-0.0077
	2017	0.0892	0.1621	0.1066	0.0173	0.0605	-0.0025

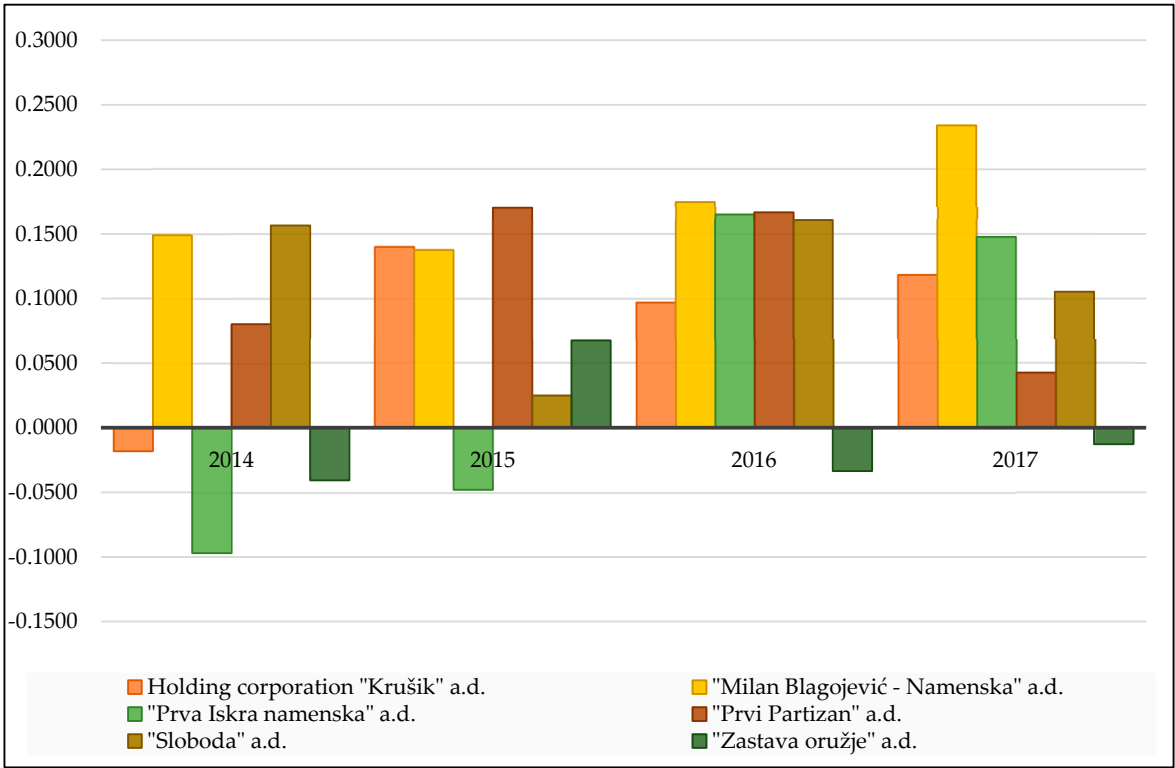
A special group called the “Defence Industry of Serbia,” which includes seven state-owned enterprises, is allocated by the Ministry of Defence (Ministry of Defence, report, 2018). These companies are HK “Krušik” a.d. Valjevo, “Milan Blagojević – namenska” a.d. Lučani, “Prva Iskra” a.d. Barič, “Prvi partizan” a.d. Užice, “Sloboda” a.d. Čačak, “Zastava oružje” a.d. Kragujevac, and “Yugoimport” SDPR (Figure 3). Beyond this group, another 216 companies, licensed for the production and trade of weapons and military equipment, cooperate closely with the dedicated defence industry (Ministry of Trade, Tourism, and Telecommunications, 2018). These companies, which include numerous institutes and faculties from the professional and academic community as subcontractors, vary in ownership structure, core business, and size. Predominantly small enterprises, and to a lesser extent medium-sized enterprises, they are mostly privately owned and collectively employ around 8,000 people.

This second segment of the Serbian defence industry includes companies primarily belonging to the metal complex, electrocomplex, and chemical complex. These entities, along with the aforementioned seven primary factories, form a robust industrial base for defence capacities. The third segment focuses on the development and enhancement of resources and comprises the Military Technical Institute, the Technical Expert Center, and three technical repair institutes within the defence system, namely the Ministry of Defence and the Army of Serbia.



**Figure 3.** Current Liquidity Ratio: A Comprehensive Measure of Financial Health and Short-term Solvency. Source: Authors.

Nowadays world is moving rapidly toward globalization, and the fact is that business performance evaluation of the defence industry’s companies through financial analysis its importance. The financial ratios involved in this research, provide useful quantitative and qualitative financial information so we can evaluate the operation of a defence industry enterprise and analyze its financial position within a sector (Figure 4).



**Figure 4.** Analysis of Business Profit Ratio. Source: Authors.

This type of analytic financial research brings awareness to managers as to which features they have to focus on. As shown in Table 1, financial analysis was carried out for 6 companies from the group "Defence Industry of Serbia" in the period from 31 December 2014 to 31 December 2017 business year, where, based on the indicators of profitability, indebtedness, liquidity and business efficiency, we can valorize the achieved results and perceive the financial position of the companies concerned. At the same time, we can also see the risk of business assets and capital, as well as the sustainability of these companies' operations.

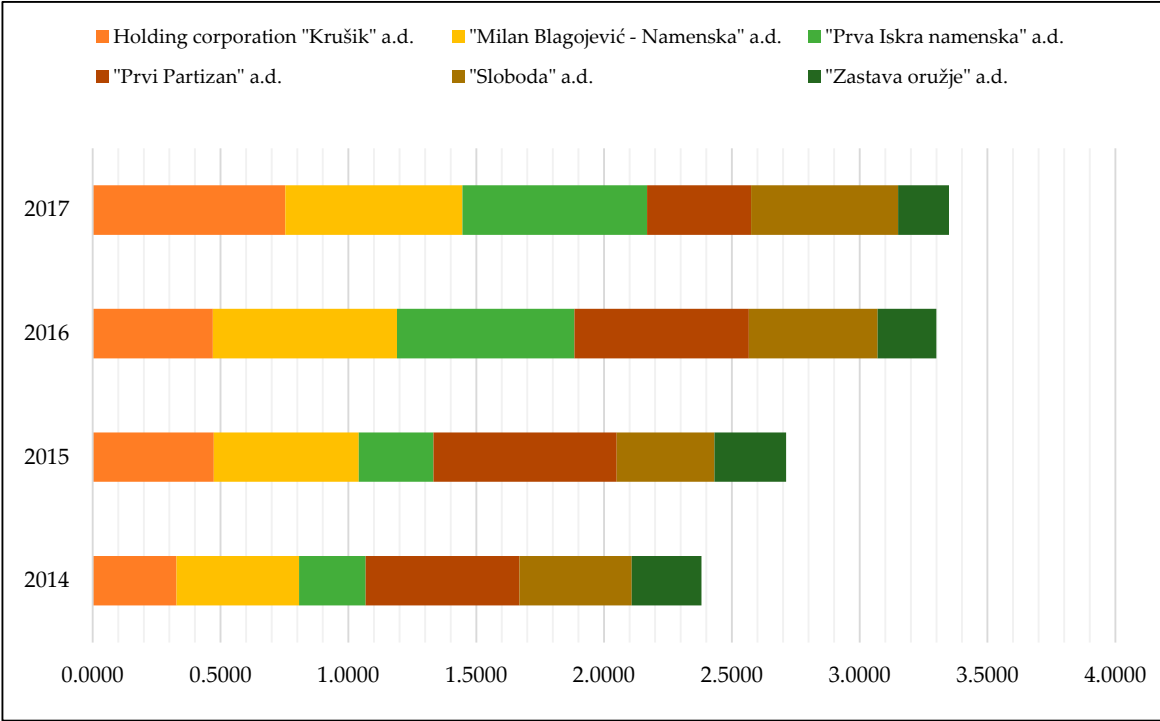
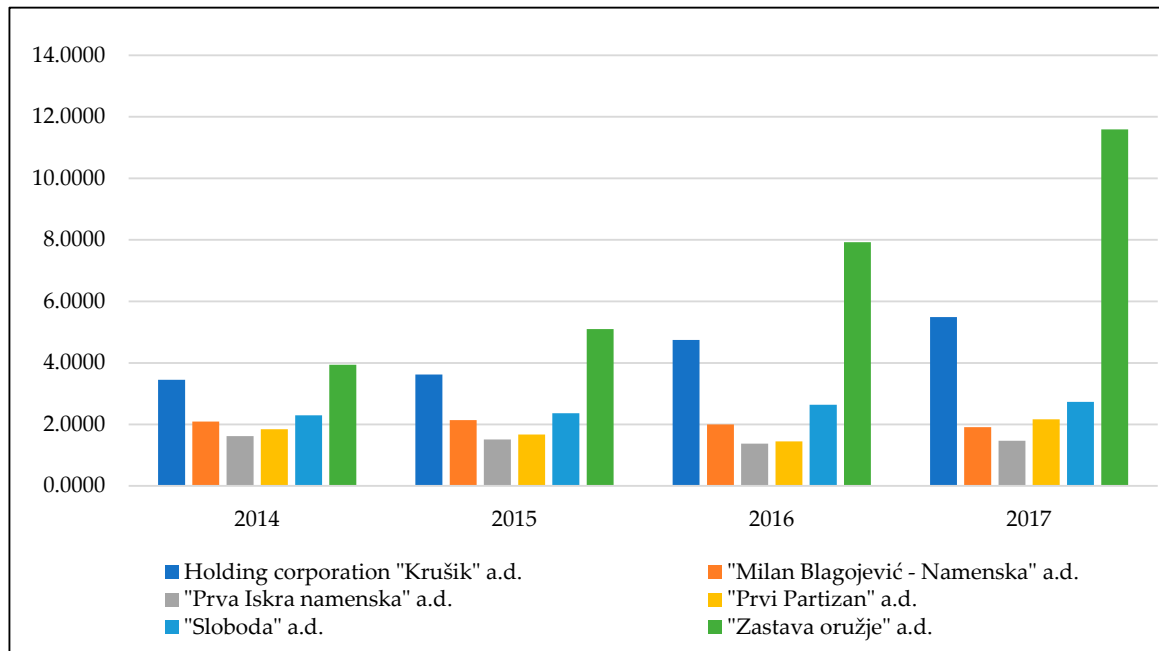


Figure 5. Total Asset Turnover Ratio Analysis. Source: Authors.

The research findings have demonstrated the impact of structural and dynamic changes in balance sheets and income statements on the business performance of the analyzed subjects. Financial ratios, serving as reliable indicators, reveal specific trends in business operations and provide critical signals for making informed business decisions within the company. These ratios not only track the historical performance but also predict future trends, enabling management to identify potential opportunities and risks. As a result, they form an essential part of the strategic decision-making process, guiding companies toward sustainable growth and operational efficiency.

The financial leverage indicator shows the value of total capital (total liabilities) supported in a monetary unit of a shareholder or own capital, and at the same time, the purposefulness of the same is reflected in the fact that it limits the excessive reliance on borrowing to minimize risk-taking in the search for higher yields. Indicator values in enterprises "Milan Blagojević-namenska" a.d. and "Prva iskra namenska" a.d. have a downward trend, with a small level of variation of value. A constant trend of growth of this coefficient was observed in "Zastava oružje" a.d., and in the other entities of the Serbian defence industry some level of variations, which is shown in Figure 6.



**Figure 6.** Leverage Analysis. Source: Authors.

The indicators return on equity - ROE and return on assets – ROA, represent the indicators of profitability, that is, the performance of the business, in which the values of these are specifically reduced to the requirement to achieve the maximum profit and return from the least engaged funds in the business process. The rate of ROE is the return on capital invested, which is obtained when the operating result is allocated to the capital, ie it is an indicator of the profitability of own capital.

This indicator shows how much profit is generated on the invested equity capital, or how much the company will earn by investing the invested funds of the shareholders. The highest level of ROE has enterprise "Krušik" a.d., then follow "Milan Blagojević – namenska" a.d. and "Prva iskra namenska" a.d. with constant growth, which indicates great business operations, and sustain development of the companies. Great variations of indicators during the researched period have "Prvi partisan" a.d., a company which had great business results in 2014 and 2015, and "Sloboda" a.d. The lowest value, as we can see in Figure 6 has "Zastava oružje" ., with constant negative results. This is due to large customer receivables, whereby current liabilities can not be settled, which in turn affects the company's final business result and income (Figure 7).

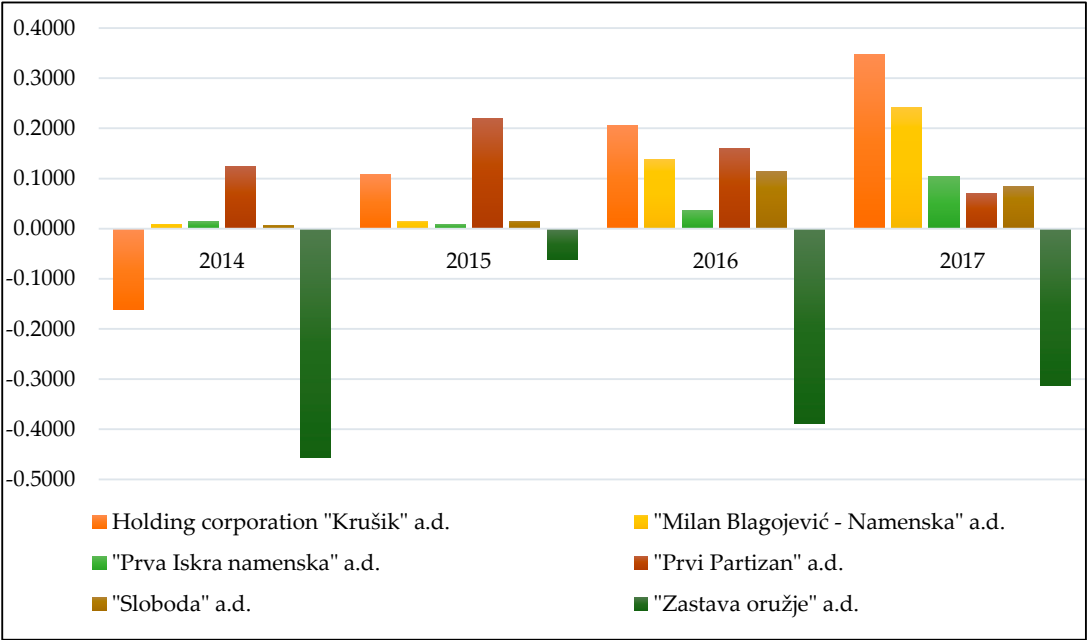


Figure 7. Return on Equity (ROE): An In-Depth Analysis.

The rate of return on total assets is the return on the invested assets, ie the total assets involved, ie the degree of efficiency. This indicator shows how much the company's management manages effectively to maximize profits (Figure 8).

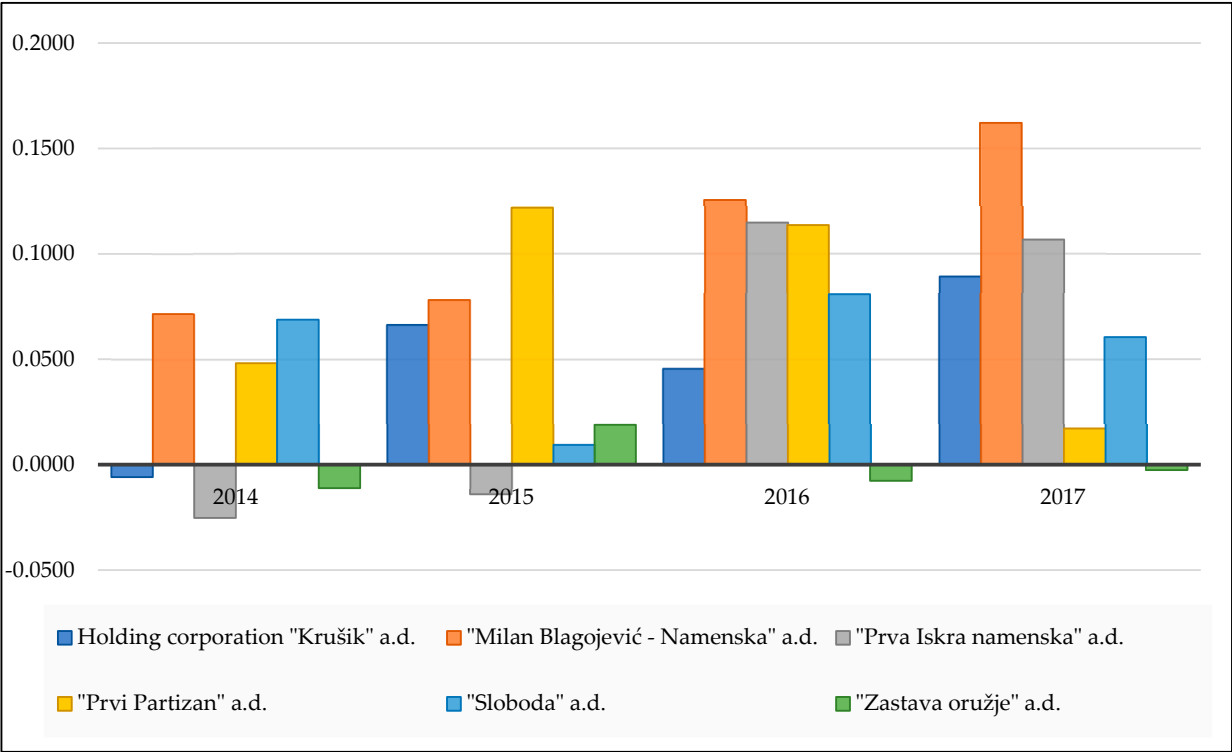


Figure 8. Return on assets (ROA). Source: Authors.



Comparative advantage is the systematization of experience in a rounded cycle of independent development and production of a wide range of assets, weapons and military equipment, as well as complex combat systems. Knowledge of standards for development and technologies for the production of Eastern and Western origin. High-quality human capital is also distinguished by dedicated industries.

As illustrated in Table 2, the analysis of employment based on annual financial statements, publicly available on the Business Registers Agency's website, reveals a notable trend. During the period from 2015 to 2017, the level of employment in the analyzed companies within Serbia's defence industry increased by approximately 30%, which is an extremely positive development. The defence industry directly employs over 10,000 individuals, and when considering its cooperative companies, this number exceeds 20,000 people. Economically, this industry's restructuring and the rising demand for both professional and junior personnel significantly benefit the entire Serbian economy by fostering sustainable development.

**Table 2.** Analysis of Employment Levels in Serbia's Leading Defence Industry Companies During the 2015-2017 Business Years.

No.		1	2	3	4	5	6	TOTAL
Company of Serbian defence industry		Holding corporation "Krušik" a.d.	"Milan Blagojević - Namenska" a.d.	"Prva Iskra namenska" a.d.	"Prvi Partizan" a.d.	"Sloboda" a.d.	"Zastava oružje" a.d.	
City		Valjevo	Lučani	Barič	Užice	Čačak	Kragujevac	
INDICATOR		Employment						
Business year	2015	1385	1121	149	933	1621	2300	7509
	2016	1922	1202	151	1541	1803	2375	8994
	2017	2615	1297	152	1546	2015	2422	10047

From the perspective of critical infrastructure security, the Serbian defence industry has made substantial efforts in recent years, drawing from past experiences and disasters. These efforts are focused on modernizing existing protection capacities, with active participation from Serbia's professional and academic communities. This modernization not only enhances the industry's resilience but also supports broader national security objectives.

#### 4. Recommendations for Enhancing the Security and Resilience of Critical Infrastructure in Serbia's Defence Industry

The following recommendations aim to bolster the security and resilience of critical infrastructure within Serbia's defence industry, ensuring robust protection and sustained functionality:

- Continuously identify, analyze, and implement incentives to justify the costs of improved security and resilience;
- Balance short-term expenses with near-term benefits to support additional investments;
- Develop market-based incentives to drive significant changes in business practices and foster markets for insurance against cyber, chemical, biological, and radiological risks;
- Support research and data collection to quantify the potential costs of inadequate infrastructure security, resilience, and cyber preparedness;
- Utilize collected data to enhance risk management strategies and enable data-driven decision-making;

- f) Establish innovation challenge programs to incentivize new solutions for infrastructure security and resilience during the planning, design, and redesign phases;
- g) Collaborate with international partners and participate in global initiatives to gain valuable insights and best practices;
- h) Apply emerging technologies such as artificial intelligence, machine learning, and big data analytics to predict and mitigate potential risks more effectively;
- i) Use these technologies for real-time monitoring, predictive maintenance, and automated response mechanisms to reduce vulnerabilities and enhance resilience;
- j) Continue national efforts in Serbia to propose a resilience assessment framework for critical infrastructures, focusing on risk assessment to address identified gaps;
- k) Ensure this framework captures interdependencies across different infrastructures, sectors, and borders, with a particular focus on resilience;
- l) Promote effective information sharing among partners to build situational awareness and enable risk-based decision-making;
- m) Foster collaboration between infrastructure owners and operators, government entities, academia, and non-profits to ensure successful risk management;
- n) Achieve consensus on common risk metrics across sectors to ensure consistency and effectiveness in measuring and managing risks;
- o) Harmonize the national risk assessment framework with EU policies and strategies for critical infrastructure;
- p) Recognize the rapid integration of the defence industry into economic flows as a vital element of Serbia's national security policy;
- q) Align with European standards and regulations, and establish preventive and control mechanisms for critical defence infrastructure to maintain Serbia's defence, security, and foreign policy interests;
- r) Develop mechanisms to protect critical infrastructure from global, regional, and internal threats, making this a national security priority for Serbia;
- s) By implementing these recommendations, Serbia can significantly enhance its efforts to secure and sustain critical infrastructure, contributing to national stability and prosperity.

By implementing these recommendations, Serbia can significantly enhance its efforts to secure and sustain critical infrastructure, contributing to national stability and prosperity.

## 5. Conclusions

The impact of infrastructure disruption is typically quantified in terms of aggregated figures that represent economic losses. This approach allows policymakers to evaluate various disruption scenarios, including cascading effects across sectors, and to assess the costs and benefits of mitigation measures (Giannopoulos et al., 2012). A comprehensive risk assessment is achievable when the impact data is combined with the likelihood of these scenarios. Without this information, the analysis remains an impact assessment and cannot effectively prioritize risk mitigation measures, especially for High Impact Low Probability (HILF) events. A significant challenge for risk assessment methodologies is to address these gaps and develop a harmonized framework at the national level, extending to the defence industry.

Such a framework should accurately capture interdependencies across different infrastructures, sectors, and borders—a critical requirement for the West Balkan countries in coordination with EU critical infrastructure policies and strategies. Additionally, there must be

consensus on a common risk metric across sectors. In summary, risk assessment for critical infrastructures should be an integral part of a broader framework, with resilience analysis as the primary tool. The continuation of this work at the national level in Serbia should focus on proposing a resilience assessment framework for critical infrastructures, where risk assessment serves as a subset to bridge the gaps identified in this research.

The social and economic stability of the world now heavily relies on the reliable supply of basic goods and services, transported and distributed through extensive technological network infrastructures. National security today depends significantly on these capacities, including the smooth functioning of the defence industry's complexes, as seen in Serbia. These critical infrastructures are subject to potential disruptive factors from hazardous natural and human environments, such as the global political climate, human capital, financial crises, severe damage, explosions in warehouses, and organized (cyber) crime or cyber warfare (Zio, 2016). The infrastructure systems within the Serbian defence industry are exposed to numerous external and internal influences, creating a potential base from which dangerous hazards and harmful events can quickly and globally spread throughout the system. This has increased systemic risk exposure, characterized by cascading failures that can significantly impact both national and regional levels. Indeed, significant disruptions have highlighted the need for the protection and resilience of critical infrastructures as a national and international priority.

In conclusion, the integrity, economic, and security stability of Serbia is closely tied to the state and developmental potential of the defence industry. Its rapid development and integration into national and international economic flows, through the acquisition of new technologies, has been recognized as a vital element of Serbia's national security policy. Aligning with European standards and regulations, and establishing preventive and control mechanisms for critical defence infrastructure, are fundamental prerequisites for maintaining the integrity of defence, security, and foreign policy interests, as well as enhancing the overall credibility of Serbia. Given the context of global, regional, and internal threats, developing adequate mechanisms for the protection of critical infrastructure has become a national security priority for Serbia.

**Funding:** This research was funded by the Scientific–Professional Society for Disaster Risk Management, Belgrade (<https://upravljanje-rizicima.com/>, accessed on 10 July 2024) and the International Institute for Disaster Research (<https://idr.edu.rs/>, accessed on 10 July 2024), Belgrade, Serbia.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Baruh, S., Dey, C., & Dutta, N. P. M. K. (2023). Dima Hasao, Assam (India) landslides' 2022: A lesson learnt. *International Journal of Disaster Risk Management*, 5(1), 1-13.
2. Bouchon S. (2006). The vulnerability of interdependent critical infrastructures systems: epistemological and conceptual state-of-the-art. Ispra, Italy: European Commission, Directorate-General Joint Research Centre, Institute for the Protection and Security of the Citizen.
3. Business Registers Agency, Financial reports of defence industry's companies, Retrieved from [www.apr.gov.rs](http://www.apr.gov.rs), accessed on 15<sup>th</sup> November 2018.
4. Carla S., R. (2019). School-community collaboration: disaster preparedness towards building resilient communities. 1(2), 45-59.
5. Carlson L., Bassett G., Buehring W., Collins M., Folga S., Haffenden B., Petit F., Phillips J., Verner D., and Whitfield R. (2012). Resilience Theory and Applications, Argonne National Laboratory, Decision and

- Information Sciences Division, ANL/DIS-12-1, Argonne, Ill., USA, Retrieved from <http://www.dis.anl.gov/pubs/72218.pdf>, accessed November 16<sup>th</sup>, 2018.
6. Carreras BA, Newman DE, Dobson I, Poole AB. (2004). Evidence for self-organized criticality in a time series of electric power system blackouts. *Circuits Syst I: Regul Pap, IEEE Trans*;51(9), pp. 1733–1740.
  7. Cimellaro GP, Reinhorn AM, Bruneau M. (2010). Framework for analytical quantification of disaster resilience. *Eng Struct*, 32(11), pp. 3639–3649.
  8. Cvetković, V. (2024). *Disaster Risk Management*. Belgrade: Scientific-Professional Society for Disaster Risk Management.
  9. Cvetković, V. (2014). Spatial and temporal distribution of floods like natural emergency situations. International scientific conference “Archibald Reiss days” Thematic conference proceedings of international significance (3-4 march 2014), Belgrade, The Academy of Criminalistic and Police Studies, 371-389, volume II.
  10. Cvetković, V. (2019). Risk Perception of Building Fires in Belgrade. *International Journal of Disaster Risk Management*, 1(1), 81-91.
  11. Cvetković, V. (2024b). Essential Tactics for Disaster Protection and Rescue. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.
  12. Cvetković, V. M. (2016). Fear and floods in Serbia: Citizens preparedness for responding to natural disaster. *Zbornik Matice srpske za drustvene nauke*, 155(2), 303-324.
  13. Cvetković, V. M. (2023). A Predictive Model of Community Disaster Resilience based on Social Identity Influences (MODERSI). *International Journal of Disaster Risk Management*, 5(2), 57-80.
  14. Cvetković, V. M., & Marković, K. (2021). Examining the Impact of Demographic and Socio-Economic Factors on the Level of Employee Preparedness for a Disaster Caused by Fires: A Case Study of Electrical Power Distribution in Serbia. *International Scientific Conference 30 Years of Independent Macedonian State 13-15 September 2021, Ohrid*.
  15. Cvetković, V. M., & Šišović, V. (2023). Capacity Building in Serbia for Disaster and Climate Risk Education. Available at SSRN 4575350.
  16. Cvetković, V. M., & Šišović, V. (2024). *Community Disaster Resilience in Serbia*. Scientific-Professional Society for Disaster Risk Management, Belgrade.
  17. Cvetković, V. M., Dragašević, A., Protić, D., Janković, B., Nikolić, N., & Milošević, P. (2022). Fire safety behaviour model for residential buildings: Implications for disaster risk reduction. *International Journal of Disaster Risk Reduction*, 102981. doi:<https://doi.org/10.1016/j.ijdr.2022.102981>
  18. Cvetković, V. M., Nikolić, N., & Lukić, T. (2024). Exploring Students’ and Teachers’ Insights on School-Based Disaster Risk Reduction and Safety: A Case Study of Western Morava Basin, Serbia. *Safety*, 10(2), 50.
  19. Cvetković, V. M., Tanasić, J., Ocal, A., Kešetović, Ž., Nikolić, N., & Dragašević, A. (2021). Capacity Development of Local Self-Governments for Disaster Risk Management. *International Journal of Environmental Research and Public Health*, 18(19), 10406.
  20. Cvetković, V. P. S., & Janković, B. (2021). Private security preparedness for disasters caused by fires. *Journal of Criminalistics and Law, NBP*, 26(1).
  21. Cvetković, V., & Filipović, M. (2017). Information systems and disaster risk management. Paper presented at the International Scientific and Professional Conference – 40 years of higher education in the field of security – Theory and Practice, Skopje, Republic of Macedonia.
  22. Cvetković, V., & Kezunović, A. (2021). Security Aspects of Critical Infrastructure Protection in Anthropogenic Disasters: A Case Study of Belgrade. *Research Squares - Preprint*, 10-21203.
  23. Cvetković, V., & Martinović, J. (2020). Innovative solutions for flood risk management. *International Journal of Disaster Risk Management*, 2(2).
  24. Cvetković, V., & Šišović, V. (2024). Understanding the Sustainable Development of Community (Social) Disaster Resilience in Serbia: Demographic and Socio-Economic Impacts. *Sustainability*, 16(7), 2620. Retrieved from <https://www.mdpi.com/2071-1050/16/7/2620>
  25. Cvetković, V., Babić, S., & Gačić, J. (2017). Religiousness level and citizen preparedness for natural disasters. *Vojno delo* 69(4):253-262
  26. Cvetković, V., Bošković, N., & Ocal, A. (2021). Individual citizens' resilience to disasters caused by floods: a case study of Belgrade. PREPRINT (Version 2) available at Research Square [<https://doi.org/10.21203/rs.3.rs-923368/v2>].

27. Cvetković, V., Nikolić, N., & Lukić, T. (2024). Exploring Students' and Teachers' Insights on School-Based Disaster Risk Reduction and Safety: A Case Study of Western Morava Basin, Serbia. *Safety*, 10(2), 2024040472.
28. Cvetković, V., Pavlović, S., & Janković, B. (2021). Private security preparedness for disasters caused by fires. *Journal of Criminalistics and Law*, NBP, 26(1), 35-59.
29. Cvetković, V., Pavlović, S., & Janković, B. D. (2021). Factors of influence on the preparedness of the private security members for fire emergencies. *NBP-Journal of Criminalistics and Law*, 26(1), 35-59.
30. Cvetković, V., Rikanović, S., & Knežević, S. (2022). The resilience of society in disasters caused by nuclear accidents. IAI International Academic Conference, 5th May 2022 at Corvinus University in Budapest, HungaryAt: Budapest, Hungary
31. El-Mougher, M. M., Abu Sharekh, D. S. A. M., Abu Ali, M., & Zuhud, D. E. (2023). Risk Management of Gas Stations that Urban Expansion Crept into the Gaza Strip. *International Journal of Disaster Risk Management*, 5(1), 13-27.
32. Frostdick, S. (1997). The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management: An International Journal*, 6(3), 165-177.
33. Giannopoulos G., Filippini R., Schimmer M. (2012). Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art, European Commission: Joint Research Centre, Institute for the Protection and Security of the Citizen, pp. 1-53.
34. Goyal, N. (2019). Disaster governance and community resilience: The law and the role of SDMA's. *International Journal of Disaster Risk Management*, 1(2), 61-75.
35. Grozdanić, G., & Cvetković, M. V. (2024). Exploring Multifaceted Factors Influencing Community Resilience to Earthquake-Induced Geohazards: Insights from Montenegro. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.
36. Hromada, M., & Lukas, L. (2012). Critical Infrastructure Protection and the Evaluation Process. *International Journal of Disaster Recovery and Business Continuity*, 3.
37. Kumiko, F., & Shaw, R. (2019). Preparing International Joint Project: Use of Japanese Flood Hazard Map in Bangladesh. *International Journal of Disaster Risk Management*, 1(1), 62-80.
38. Law on Critical Infrastructure (2018), Official Gazette of the Republic of Serbia, no. 87/18.
39. Lewis TG. (2006). Critical infrastructure protection in homeland security: defending a networked nation, Wiley.
40. Mano, R., A, K., & Rapaport, C. (2019). Earthquake preparedness: A Social Media Fit perspective to accessing and disseminating earthquake information. *International Journal of Disaster Risk Management*, 1(2), 19-31.
41. Ministry of Defence, Report of the defence industry of the Republic of Serbia, Retrieved from www.mod.gov.rs on 29<sup>th</sup> November 2018.
42. Ministry of Trade, Tourism and Telecommunications (2018). Report and list of persons registered for foreign trade in weapons and military equipment, Retrieved from www.mtt.gov.rs, on 2<sup>nd</sup> November 2018.
43. Moteff JD. (2012). Critical infrastructure resilience: the evolution of policy and programs and issues for congress. *Congr Res Serv*/12.
44. Murray, A. T., & Grubescic, T. H. (2012). Critical infrastructure protection: The vulnerability conundrum. *Telematics and informatics*, 29(1), 56-65.
45. Nikčević S. (2009). Security integration and the Serbian defence industry. *Chance for sustainable development. Economics and Security*, Center for Civil-Military Relations, Belgrade, pp. 169-179.
46. Obama B. (2013). Presidential policy directive 21: critical infrastructure security and resilience. Washington, DC, U.S.
47. Öcal, A. (2019). Natural Disasters in Turkey: Social and Economic Perspective. *International Journal of Disaster Risk Management*, 1(1), 51-61.
48. Perić, J., & Cvetković, V. M. (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), 31-45.
49. Petit F., Verner D., Brannegan D., Buehring W., Dickinson D., Guziel K., Haffenden R., Phillips J., Peerenboom J. (2015). Analysis of critical infrastructure dependencies and interdependencies. *Risk and Infrastructure Science Center, Global Security Sciences Division, Argonne National Laboratory*.



50. Petit F.D., Bassett G.W., Buehring W.A., Collins M.J., Dickinson D.C., Haffenden R.A., Huttenga A.A., Klett M.S., Phillips J.A., Veselka S.N., Wallace K.E., Whitfield R.G., and Peerenboom J.P., (2013). Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-13-04, Argonne, Ill., USA, Retrieved from <http://www.ipd.anl.gov/anlpubs/2013/11/77931.pdf>, accessed November 5<sup>th</sup>, 2018.
51. Radić N., Radić V. (2018). Foreign Direct Investments in the Defence Industry of Serbia, *Military Work* 5/18, pp. 163-190.
52. Radić V., Radić N. (2018). Economic Aspects and National Self-Sufficiency of the Defence Industry of Serbia, *Military Work* Vol. 70, No. 4, pp. 162-179.
53. Rajani, A., Tuhin, R., & Rina, A. (2023). The Challenges of Women in Post-disaster Health Management: A Study in Khulna District. *International Journal of Disaster Risk Management*, 5(1), 51-66.
54. Rinaldi S.M., Peerenboom J.P., Kelly T.K. (2001). Complex Networks, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, *IEEE Control Systems Magazine*, December 2001, pp. 11–25.
55. Škero, M., & Ateljević, V. (2015). Protection of critical infrastructure and basic elements of compliance with Council Directive 2008/114 / EC. *Vojno delo*, 67 (3), 192-207.
56. Sudar, S., Cvetković, V., & Ivanov, A. (2024). Harmonization of Soft Power and Institutional Skills: Montenegro's Path to Accession to the European Union in the Environmental Sector. *International Journal of Disaster Risk Management*, 6(1), 41-74.
57. U.S. Department of Homeland Security - DHS (2013). NIPP 2013 – Partnering for Critical Infrastructure Security and Resilience, Retrieved from [https://www.dhs.gov/sites/default/files/publications/NIPP%202013\\_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience\\_508\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf), accessed November 17<sup>th</sup>, 2018.
58. Vibhas, S., Bismark, A. G., Ruiyi, Z., Anwaar, M. A., & Rajib, S. (2019). Understanding the barriers restraining the effective operation of flood early warning systems. *International Journal of Disaster Risk Management*, 1(2), 1-19.
59. Xuesong, G., & Kapucu, N. (2019). Examining Stakeholder Participation in Social Stability Risk Assessment for Mega Projects using Network Analysis. *International Journal of Disaster Risk Management*, 1(1), 1-31.
60. Zio E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures, *Reliability Engineering and System Safety*, pp. 137-150.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.