Ivana Pokrajčić
Ministry of Defense of the Republic of Croatia
University of Defense and Security "Dr. Franjo Tuđman", Croatia
E-mail: ivana.pokrajcic@sois-ft.hr

Tonći Lazibat
Full professor
University of Zagreb, Faculty of Economics and Business, Croatia
E-mail: tlazibat@net.efzg.hr

REGULATORY PRESSURE AND ORGANIZATIONAL COMPLIANCE IN NATIONAL CRITICAL INFRASTRUCTURE: IMPLICATIONS FOR RISK MANAGEMENT AND OPERATIONAL RESILIENCE

Preliminary communication
UDK: 351.86:005.334](497.5)
JEL classification: H54, H12, H56, G32, K23
https://doi.org/10.17818/DIEM/2026/SI2
Paper received: March 9, 2026
Paper accepted: July 14, 2026

Abstract

The protection of national critical infrastructure plays a central role in maintaining national security, economic stability, and public welfare. This research investigates perception of regulatory pressure and the requirements for operational resilience and risk management under current regulatory frameworks among 55 companies within national critical infrastructure sectors. Methodology combines an anonymous online survey with semi-structured interviews to capture both quantitative trends and qualitative insights. Descriptive statistics were used to analyse survey responses, while interviews offered a deeper understanding of sector-specific practices and organizational attitudes. The results show significant differences in perception of regulatory pressure and establishment of risk management priorities among the sectors of critical infrastructure, and also highlight the persistent gap between regulatory intent and organizational behavior.

Keywords: critical infrastructure, risk management, resilience, regulatory compliance

1. INTRODUCTION

National critical infrastructure (NCI) forms the backbone of a country s security, economic stability, and public welfare. Its uninterrupted functioning is essential for maintaining societal continuity, and disruptions can have wide-ranging economic and social consequences. The European Union (EU) has emphasized the protection of critical infrastructure through Critical Entities Resilience Directive from which establishes a framework for identifying European critical infrastructures and assessing the need to enhance their protection. Croatia has implemented these principles through the Law on Critical Infrastructure (Republic of Croatia, 2025). Associated regulations, including the Decision on the Designation of Sectors and Lists of Priority Sectors of Critical Infrastructure (Republic of Croatia, 2013) still remain to be written to reflect the new law. Complementary guidance, such as the Ministry

of the Interior s Regulation on the Methodology for Conducting Risk Analyses of Critical Infrastructure Operations (Republic of Croatia, 2016), aligned with ISO 31000:2009 (International Organization for Standardization, 2009), provides structured procedures for identifying, assessing, and mitigating risks. Together, these instruments aim to ensure continuity of operations, minimize the impact of disruptions, and protect the population and the economy of the nation.

Risk assessment for NCI typically combines quantitative and qualitative methods (Renda, 2010). Quantitative approaches estimate the probability and potential impact of disruptions, while qualitative methods address less tangible threats, such as cyberattacks, political instability, or social unrest (Barker et al., 2025). Recent research has shifted focus toward resilience, defined as the ability of NCI systems to maintain operations during and after disruptive events. Corporate operators are pivotal in safeguarding NCI, particularly since many critical assets are privately owned, while regulatory oversight rests with government agencies. Some companies view compliance with legal frameworks as a means to strengthen resilience and risk management, while others see it as an administrative or financial burden. The aim of this article is to analyse the perception of regulatory pressure among organizations within national critical infrastructure sectors and to assess its influence on the development of risk management practices and operational resilience, with particular attention to sectoral differences and the alignment between regulatory frameworks and organizational behavior (Pokrajčić, 2025). The article is structured as follows: After the introductionary chapter, chapter 2 examines the critical infrastructure of the Republic of Croatia, with particular emphasis on the specific features of risk management and resilience within NCI. Chapter 3 presents the methodological framework and the results of the empirical research, including both quantitative and qualitative findings across NCI sectors. Finally, Chapter 4 offers concluding remarks and discusses the key implications of the research.

2. CRITICAL INFRASTRUCTURE OF THE REPUBLIC OF CROATIA

Critical infrastructure encompasses the systems, networks, and assets that are essential for the functioning of the state and society as a whole (Akrap, 2019). At its foundation, it consists of systems, networks, and facilities that maintain societal stability and continuity by supporting key sectors such as the economy, security, and public services. According to Alcatraz and Zaedally (2015), critical infrastructure includes both physical and logical components that are vital for the minimum functioning of government administration and economic systems.

In Croatia, NCI includes essential systems, facilities, and services whose failure would have serious repercussions for national security, the economy, public health, or citizen safety. Recognized as a cornerstone of national prosperity, Croatia's critical infrastructure was first formally defined and regulated under the Law on Critical Infrastructure (Republic of Croatia, 2013; Republic of Croatia, 2022), while the new law was published on 13 June 2025 (Republic of Croatia, 2025).

Through its legal framework, the Republic of Croatia seeks to ensure adequate protection of NCI, promote cooperation among various stakeholders, and enhance the resilience of critical infrastructure sectors against diverse threats and challenges. This legal framework represents a key instrument for strengthening national security and stability. In Croatia, in addition to the legislative framework previously described, the Regulation on the Methodology for Conducting Risk Analyses of National Critical Infrastructure Operations (Republic of Croatia, 2016) establishes guidelines, criteria, and metrics for identifying critical infrastructure and conducting risk analyses. This document specifies the responsibilities of the risk analysis owners and defines the procedures for carrying out risk assessments, which form an integral part of the overall risk management process. These guidelines and criteria for risk analysis are aligned with the ISO 31000:2009 risk management standard, and it is expected that the new version will be aligned with the updated ISO 31000:2018 (International Organization for Standardization, 2018).

As part of the regulation, a decision on numerical and descriptive indicators for intersectoral criteria for risk analysis and critical infrastructure identification was issued (Trut, 2021:198). The regulation states that the owners responsible for conducting sectoral risk analyses must collaborate and exchange data with risk analysis owners from other sectors and with infrastructure owners/operators. This is essential for understanding interdependencies, associated risks, and vulnerabilities across different critical infrastructure sectors.

2.1. Specific Features of Risk Management in Subjects within the NCI

Security risk management within the NCI segment is high priority, as these systems are increasingly exposed to a wide range of threats. Despite significant advances in protective measures, NCI continues to face several challenges in effective risk management.

One of the primary challenges is the growing complexity of infrastructure systems. As infrastructure becomes more technologically advanced, it also becomes more interconnected and interdependent. According to Wells et al. (2022), the integration of physical and cyber systems has created a highly complex environment where threats affecting one sector can cascade into others. Modern infrastructure often includes legacy systems that were not designed to withstand contemporary security threats. Challenges in upgrading these systems – due to costs, regulatory constraints, and technical limitations – further complicate security risk management (Avery & Ranganathan, 2016). Additionally, the lack of standardized security protocols across different infrastructure sectors adds complexity, as agencies and private operators may have varying levels of preparedness and response capabilities.

Since NCI is largely privately owned and operated, while government agencies oversee regulatory compliance and national security, a significant challenge lies in the insufficient collaboration between public and private sectors. Mayer & Lu (2025) note that private companies often hesitate to share sensitive information regarding vulnerabilities or incidents due to concerns over reputational damage, legal consequences, or financial losses. This lack of transparency can delay threat identification and mitigation, leaving infrastructure more vulnerable to attacks. On the other side, public sector institutions may lack the resources or technical expertise necessary to fully understand the specific risks faced by private companies. This disconnect between sectors hinders the development of coherent and effective risk management strategies. Another significant challenge is the complexity of regulatory and legal frameworks. National security is often governed by a patchwork of laws and policies that differ across sectors and jurisdictions. Such fragmentation can lead to inconsistencies in risk management standards and create uncertainties regarding accountability in the event of security incidents (Barker et al,, 2025). Furthermore, the complexity of managing security risks in the NCI segment requires a coordinated approach among numerous organizations, agencies, and sectors. Bureaucratic inefficiencies, unclear roles and responsibilities, and lack of inter-organizational coordination can disrupt effective risk management. Absence of alignment, combined with poor communication and accountability, may delay responses to security incidents and miss opportunities to prevent escalation (Wells et al., 2022).

In summary, security risk management in Croatia's NCI faces numerous challenges arising from the complexity of modern systems, lack of public-private collaboration, evolving threats, fragmented regulatory and legal frameworks, human factors, and sectoral interdependencies (Pederson et al., 2006:5). Addressing these challenges requires integrated, multidisciplinary strategies that combine technological, organizational, and legal approaches to enhance resilience and continuity of operations.

2.2. Resilience of NCI

Resilience factors are critical to the ability of NCI to recover rapidly and adapt to changes. Rehak et al. (2018:5) emphasize both technical resilience (robustness and recovery capability) and organizational resilience (adaptability) across sectors such as energy, information and communication technology, and transport, illustrating resilience through case studies under various conditions. The main conclusions of Rehak et al. (2018:3) highlight the importance of investing in NCI resilience, focusing on two key domains: technical resilience and organizational resilience. The authors stress that technical factors (such as robustness and recoverability) and organizational factors (such as adaptability and preparedness) jointly enhance a system's ability to withstand disruptions and recover quickly. Thamboo et al. (2022) provide a systematic review of models for assessing critical infrastructure resilience, with a particular focus on natural disasters. Kramer (2021) analyzed the impact of the COVID-19 pandemic on critical infrastructure resilience, recommending adaptive frameworks that integrate crisis management across all NCI sectors. Yang et al. (2024), examining resilience in healthcare and transport sectors, classify cascading impacts into four scenarios, regardless of whether effects occur within or beyond a specific infrastructure system. Tundys (2023) analysed implications and consequences of incidental disruptions and black swan phenomena in the supply chains, arguing that being aware of the risks, it is necessary to take measures to minimise the risk of their occurrence or to minimise the possible effects of, for ripple effects (Thundys, 2023:167). The literature clearly indicates a consensus on the need for an integrated approach to strengthening NCI resilience, combining technical protective measures with adaptive risk management strategies to achieve long-term robustness (Kaaleva, 2025; Pokrajčić & Lazibat, 2025).

Understanding how companies within the NCI segment perceive legal obligations and resilience requirements is essential for assessing the effectiveness of regulatory frameworks, particularly in light of the new law. Research conducted across key NCI sectors focused on how private and public companies interpret, prioritize, and implement compliance measures, as well as how they integrate resilience into operational practices (Rehak et al., 2018; Thamboo et al., 2022; Kramer, 2021).

Earlier research reported diverse perceptions of legal pressure arising from the lawmakers and related regulations. While some organizations view compliance as a clear mandate and a driver for structured risk management (Hemme, 2015), others perceive regulatory requirements as complex, burdensome, or ambiguous, particularly where overlapping sectoral and cross-border legislation exists (Yang et al., 2024). This divergence reflects differences in organizational resources, experience with risk management, and sectoral exposure to threats (Avery & Ranganathan, 2016; Pederson et al., 2006).

3. METHODOLOGY AND RESEARCH RESULTS

To explore how the 2025 Croatian Critical Infrastructure Law influences enterprise practices, this article examined how companies from critical infrastructure sectors perceive legal obligations, prioritize compliance, and implement resilience measures within their operational frameworks.

3.1. Methodological Approach

The research was conducted among 55 companies operating within sectors of Croatia s national critical infrastructure. An anonymous online survey was employed to collect data on how companies perceive legal obligations under the 2025 Croatian Critical Infrastructure Law and how they integrate resilience measures into their operational practices. In addition to the survey instrument, a semi-structured interview approach was conducted to collect qualitative insights. Respondents answers were systematically recorded and categorized according to their respective NCI sectors, enabling

sector-based comparison and interpretation of findings. The sample of companies was generated using publicly available databases, including the Digital Chamber of Commerce service (HGK – Croatian Chamber of Commerce) and info.BIZ (FINA – Financial Agency).

Respondents expressed their views using a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) on statements related to perceived legal obligations.. For descriptive statistical analysis, the arithmetic mean and standard deviation were used for interval-scale variables. Distributions were further examined by determining minimum and maximum values, as well as skewness and kurtosis coefficients. The normality of distributions was tested using the Kolmogorov-Smirnov test, ensuring the appropriateness of subsequent statistical analyses. The distribution of the total of 49 collected responses is shown in Table 1.

Table 1 The Distribution of Respondents in the Sectors of NCI

	Energy	Digital Infrastructure	Transport	Health	Water management	Food production	Banking	Public services
Number of respondents	7	5	6	3	9	11	4	4

Source: Author

The perceived effect of regulatory pressure was measured using a set of statements adapted from validated instruments developed by Bulgurcu et al. (2010), Siponen et al. (2007), and Straub (1990). The statements captured multiple dimensions of regulatory pressure, including perceived imposition of security risk management requirements, personal accountability toward supervisory authorities, oversight intensity, and perceived consequences of non-compliance.

3.2. Quantitative Research Results

The results of the survey indicate variation in how companies perceive regulatory and legal pressures related to the 2025 Critical Infrastructure Law. The arithmetic mean and standard deviations of responses across sectors is summarized in Table 2.

Table 2 Arithmetic Means and Standard Deviations of Collected Results Across the Sectors

NCI Sector	N	M	SD	Interpretation of Perceived Regulatory Pressure
Energy	7	1.43	0.79	Very low perceived pressure; compliance seen as manageable and integrated into operations.
Digital Infrastructure	5	1.80	0.84	Low perceived pressure; regulatory obligations are understood and not seen as burdensome.
Transportation	6	2.33	0.52	Moderate perceived pressure; mixed perceptions of compliance complexity across organizations.
Healthcare	3	2.67	0.58	Moderate to somewhat high pressure; responsibilities for compliance and risk management perceived as significant.
Water Management	9	3.22	0.44	High perceived pressure; regulations viewed as demanding due to interdependencies and technical challenges.
Food Production	11	3.27	0.47	High perceived pressure; compliance considered substantial and impactful on operations.
Banking	4	1.50	0.58	Very low perceived pressure; obligations are clear, well-structured, and well-supported by oversight.
Public Services	4	1.75	0.50	Low perceived pressure; strong regulatory culture and established procedures reduce perceived burden.

Source: Author

Companies in the energy sector reported the lowest perceived regulatory pressure, with M=1.43 and SD=0.79. This suggests that respondents strongly disagree with the notion that regulatory obligations are burdensome or imposed unnecessarily. It may reflect well-established compliance procedures, structured risk management practices, and previous experience with regulatory oversight, which allow these companies to integrate legal requirements smoothly into operations. Similarly, companies in the digital infrastructure sector reported low perceived pressure (M = 1.80). Responses indicate that most respondents do not view compliance as overly demanding, likely due to the sector s familiarity with cybersecurity regulations and continuous monitoring frameworks. Transportation companies reported moderate perceived pressure (M=2.33, SD=0.52), indicating a mixed perception of regulatory obligations. Healthcare sector respondents reported slightly higher perceived pressure (M= 2.67, SD=0.58), suggesting a tendency toward viewing regulations as moderately demanding. Given the sector s exposure to both operational and public health risks, these companies may perceive higher responsibility and accountability for ensuring compliance, contributing to a stronger sense of regulatory pressure. Water management companies reported the highest perceived regulatory pressure,(M=3.22, SD=0.44). This indicates that respondents agree that regulatory obligations potentially burdensome. This perception could result from complex interdependencies with other sectors or limited resources. Similarly, the food production sector showed a high mean (M=3.27, SD=0.47), reflecting that companies perceive regulatory requirements as substantial and impactful on operations. This could be due to sector-specific compliance standards, safety regulations, and risk mitigation obligations, especially given the potential societal impact of disruptions. Banking sector respondents reported low perceived regulatory pressure (M=1.50, SD=0.58), indicating that compliance is well-integrated within operational procedures. This may be attributed to the longstanding regulatory culture and strictly established frameworks in the financial sector. Companies providing public services also reported low perceived pressure (M=1.75, SD=0.50), suggesting that they perceive regulatory obligations as clear, well-structured, and not perceived as a pressure.

The survey highlights sector-specific differences in the perception of regulatory and legal pressure. Sectors such as energy, digital infrastructure, banking, and public services perceive minimal regulatory burden, whereas water management and food production report higher perceived pressure. These variations may reflect differences in organizational resources, regulatory complexity, interdependencies with other sectors, and the maturity of risk management practices (Rehak et al., 2018; Thamboo et al., 2022; Kramer, 2021; Yang et al., 2024). The results suggest that while the 2025 Croatian Critical Infrastructure Law establishes uniform obligations across sectors, the subjective experience of regulatory pressure varies, with operational and resource-intensive sectors reporting greater perceived demands.

3.3. Qualitative Research Results across the Sectors of NCI

3.3.1. Energy Sector

The energy sector represents one of the most critical components of NCI, as its stable operation and resource availability directly condition the functionality of all other infrastructure sectors. Interview participants from the energy sector consistently emphasized this interdependence, noting that disruptions in energy supply would immediately propagate across transport, water supply, telecommunications, healthcare, and emergency services. Croatia's reliance on a diversified energy mix was frequently cited by respondents as a strategic advantage, but also as a source of increased system complexity and exposure to sector-specific risks.

Participants highlighted that the security dimension of the energy sector extends beyond operational continuity to encompass both physical and organizational security measures. In line with Alispahić et al. (2015:482), respondents described physical security as protection against terrorist threats, natural disasters, technical failures, and human error.

Respondents also demonstrated a high level of awareness of national strategic documents and they acknowledged that the regulatory and institutional framework governing critical infrastructure protection has contributed to greater awareness of security and resilience requirements within the energy sector.

3.3.2. Digital Infrastructure Sector

Interviews with representatives from seven companies within the Digital Infrastructure sector highlighted a generally low perception of regulatory pressure, consistent with the survey results. Respondents frequently emphasized that compliance with the 2025 Croatian Critical Infrastructure Law and related cybersecurity regulations is well-integrated into their standard operational procedures. Several participants noted that regulatory requirements are clear and predictable, allowing them to proactively align risk management and resilience measures without significant disruption to daily operations.

A few respondents expressed that oversight from regulatory bodies, while present, is largely supportive rather than punitive. For example, one IT infrastructure manager explained, "We receive guidance and feedback from authorities, but there is no sense that compliance is an additional burden; it's part of how we operate every day." Another participant noted that their existing cybersecurity frameworks and internal risk management practices often exceed legal requirements, reducing the perception of external pressure.

Nonetheless, some interviewees mentioned challenges arising from rapid technological changes and evolving cyber threats, which require constant adaptation. While the legal framework itself is not seen as burdensome, companies highlighted that maintaining resilience in the face of new threats sometimes demands investments in staff training, monitoring tools, and infrastructure upgrades. These requirements are perceived as operational necessities rather than externally imposed pressures, aligning with the sector's overall low perceived regulatory burden.

3.3.3. Transportation Sector

Interviews with representatives from transportation companies revealed a moderate perception of regulatory pressure, in line with the survey results. Respondents generally acknowledged the importance of complying with the 2025 Croatian Critical Infrastructure Law and related safety and risk management regulations, but many indicated that meeting these requirements can be complex due to the sector's operational and interdependent nature.

Several participants highlighted challenges related to coordination across multiple modes of transport – road, rail, and ports – as well as the integration of new safety and cybersecurity measures into existing infrastructure. Some respondents also reported that limited resources and staff experience in risk management amplify the perceived complexity of compliance, particularly for smaller companies within the sector.

Despite these challenges, interviewees generally recognized that regulatory oversight encourages structured risk management practices, including regular audits, safety drills, and contingency planning. The pressure is therefore perceived as a motivator for operational improvement rather than an arbitrary requirement.

3.3.4. Healthcare Sector

Interviews with healthcare providers revealed a moderate to somewhat high perception of regulatory pressure. Respondents recognized the critical role of compliance with the law, particularly regarding patient safety, operational continuity, and cyber-physical security. A hospital IT manager

stated, "We have multiple layers of compliance to meet – cybersecurity, data protection, and operational continuity – and it often feels challenging to stay ahead."

Participants highlighted that coordination between administrative, clinical, and technical staff is necessary to implement regulations effectively, and this creates an additional operational burden. Despite this, most respondents viewed the regulatory framework as an essential driver for structured risk management and resilience planning, ensuring the hospital systems can continue operating during disruptions or emergencies.

3.3.5. Water Management Sector

Respondents from water management organizations expressed higher perceived regulatory pressure, reflecting both the criticality of water services and the technical complexity of infrastructure. Interviewees emphasized that compliance requirements are extensive, covering operational safety, emergency preparedness, and interdependencies with energy and transportation sectors.

Participants od the interview indicated that regulations are strict, and non-compliance can have serious consequences, not just for the company but for entire communities. Participants also reported that small margins for error, aging infrastructure, and the need for rapid adaptation to regulatory updates increase the perception of pressure.

3.3.6. Food Production Sector

Interviews with food production companies indicated high perceived pressure from regulatory frameworks. Respondents acknowledged that compliance spans food safety, supply chain continuity, and critical infrastructure obligations, which can be resource-intensive.

One respondent noted, "We have to balance production efficiency with multiple layers of compliance. It feels like regulatory pressure is constant, but it also pushes us to improve our systems and processes." Interviewees also highlighted challenges in aligning internal processes with both sector-specific regulations and cross-sector critical infrastructure requirements and interdependency with transportation and energy sectors further which amplified the perception of pressure.

3.3.7. Banking Sector

Banking sector representatives reported low perceived regulatory pressure, consistent with the survey mean. Participants emphasized that compliance culture is well-established, and internal risk management and resilience practices are largely aligned with regulatory expectations.

As per interview conclusions, banking sector already operates under strict regulations, so the Critical Infrastructure Law doesn't feel like an additional burden, but it mostly confirms what they already do. Some respondents noted that while compliance is rigorous, it is perceived as manageable and integrated into daily operational practices.

3.3.8. Public Services Sector

Public service organizations also reported low perceived regulatory pressure. Respondents indicated that clear guidance, structured oversight, and dedicated support from central authorities make compliance straightforward and routine.

Overall, the responses from interview participants stated that the procedures are well-documented, and there is a clear line of responsibility, and negated any pressure from the regulatory bodies. Participants highlighted that the focus on resilience planning and risk management is well-supported institutionally, reducing the perception of burden.

4. CONCLUSION

The findings of this research reveal that companies within Croatia's NCI sectors perceive regulatory pressure and resilience requirements in varying ways, influenced by sector-specific characteristics, organizational resources, and exposure to potential threats. Sectors such as water management and food production reported higher perceived regulatory pressure, reflecting the operational complexity, interdependencies with other infrastructure sectors, and the potentially significant societal impact of disruptions. In contrast, banking and public service organizations indicated relatively lower perceived pressure, likely due to the integration of compliance measures into existing risk management frameworks and strong institutional support.

The research also highlighted notable differences in the practical implementation of security risk management. During interviews with representatives of NCI companies, it became clear that authorities emphasize the prioritization of security risks over business risks. However, in practice, this is not consistently observed. Companies remain primarily profit-driven, treating operational business risks as higher priorities. Legislative mandates appear to be the main driver for formally integrating security risk prioritization into operational practices.

These results underscore the need for tailored regulatory strategies, sector-specific guidance, and stronger incentives for private companies to align operational priorities with national security objectives. While the 2025 Croatian Critical Infrastructure Law provides a legal framework for risk management and resilience, its effectiveness depends on how organizations incorporate these requirements into daily decision-making, balancing legal obligations with practical business considerations.

Future research should investigate mechanisms for bridging the gap between regulatory intent and enterprise practice, including public-private collaboration, risk-awareness training, and incentive-based compliance strategies. Addressing these challenges is essential for enhancing the resilience of Croatia's NCI sectors and ensuring the continuity of critical services under complex and unpredictable threat scenarios.

Author Contributions: Conceptualization: I.P.; Methodology, I.P.; Formal Analysis, I.P.; Writing – Original Draft Preparation, I.P.; Writing – Review & Editing, T.L.; Supervision, T.L.

Funding: The research presented in the manuscript did not receive any external funding.

Conflict of interest: None.

Acknowledgement of AI or AI-assisted tools use: During the preparation of this paper, the author(s) used ChatGPT to format the reference list in accordance with APA style and Google Translate to assist with translating the text into English and to ensure consistency in wording and terminology.

REFERENCES

Akrap, G. (2019). Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura. *Strategos*, *3*(2), 37-49. https://hrcak.srce.hr/231009

Alcatraz, C. & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

Alispahić, B., Kovačević, G. & Korajlić, N. (2015). Značaj kritične infrastukture u sustavu nacionalne sigurnosti (2015). *8. međunarodna znanstveno-stručna konferencija „Dani kriznog upravljanja :zbornik radova*. Velika Gorica: Veleučilište Velika Gorica. https://www.researchgate.net/publication/338491599

Avery, A. & Ranganathan, C. (2016). Financial performance impacts of information security breaches. *WISP Proceedings, 6*. https://aisel.aisnet.org/wisp2016/6

Barker, K., Bessarabova, E., Radhakrishnan, S., González, A. D., Weber, M. S., Marquez, J. E. R., Vorobeychik, Y., & Jiang, J. N. (2025). Risk analysis of disinformation weaponized against critical networks. *Risk Analysis*, *45*, 4088–4096. https://doi.org/10.1111/risa.70062

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548. https://doi.org/10.2307/25750690

European Parliament and Council of the EU. (2022). *Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Directives 2016/1148 and 2018/1972, and repealing Directive 2016/1148* (NIS2 Directive 2022/2555). Official Journal of the EU, L 337, 1–99. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:337:FULL

European Parliament and Council of the EU. (2016). *Directive of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union* (NIS Directive 2016/1148). Official Journal of the EU, L 194, 1–30. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:194:FULL&from=PL

Hemme, K. (2015). Critical infrastructure protection: Maintenance is national security. *Journal of Strategic Security*, *8*(3), 25-39. http://dx.doi.org/10.5038/1944-0472.8.3S.1471

International Organisation for Standardisation. (2009). *Risk Management - Guidelines* (ISO Standard No. 31000:2009). https://www.iso.org/standard/43170.html

International Organisation for Standardisation. (2018). *Risk Management - Guidelines* (ISO Standard No. 31000:2018). https://www.iso.org/standard/65694.html

Kaaleva, T. (2025). Enhancement of critical infrastructure resilience. *Security Science Journal*, *6*(2), 218-232. https://doi.org/10.37458/ssj.6.2.10

Kramer, F. D. (2021). *Effective resilience and national strategy: Lessons from the pandemic and requirements for key critical infrastructures.* Atlantic Council. https://www.atlanticcouncil.org

Mayer, M., & Lu, Y. C. (2025). Global structures of digital dependence and the rise of technopoles. *New Political Economy, 30*(5), 755–774. https://doi.org/10.1080/13563467.2025.2497766

Pederson, P., Dudenhoeffer, D., Hartley, S. & Permann, M. (2006). *Critical infrastructure interdependency modeling: a survey of US and international research*. Idaho National Laboratory. https://inldigitallibrary.inl.gov/sites/sti/sti/3489532.pdf

Pokrajčić, I. (2025). Bihevioralni pristup upravljanju sigurnosnim rizicima: rezultati empirijskog istraživanja. P*oslovna izvrsnost - Business Excellence*, *19*(2), 37-55. https://doi.org/10.22598/pi-be/2025.2.37620

Pokrajčić, I. & Lazibat, T. (2025). The correlation between the implementation of ISO 31000:2018 and the maturity of security risk management in companies from the national critical infrastructure sector of the Republic of Croatia. *Ekonomska misao i praksa, 34*(2), 369-394. https://doi.org/10.17818/EMIP/2025/26

Rehak, D., Senovsky, P., & Slivkova, S. (2018). Resilience of critical infrastructure elements and its main factors. *Systems*, *6*(2), 1-13. https://doi.org/10.3390/systems6020021

Renda, A. (2010). *Protecting critical infrastructure in EU: CESP Task Force Report*. Center for European Policy Studies. https://cdn.ceps.eu/wp-content/uploads/2010/12/Critical Infrastructure Protection Final A4.pdf

Republic of Croatia. (2013). *Decision on the determination of sectors from which central state administration bodies identify national critical infrastructures and the list of priority sectors of critical infrastructure* (Narodne novine, 108/2013). https://narodne-novine.nn.hr

Republic of Croatia. (2016). *Regulation on the methodology for conducting risk analyses of critical infrastructure operations* (Narodne novine, 47/2016). https://narodne-novine.nn.hr

Republic of Croatia. (2017). *National security strategy of the Republic of Croatia* (Narodne novine, 73/2017). https://narodne-novine.nn.hr

Republic of Croatia. (2025). *Law on critical infrastructure* (Narodne novine, 89/2025). https://narodne-novine.nn.hr

Siponen, M., Pahnila, S. &Mahmood, A. (2007). Employees 'adherence to information security policies: An empirical study. In: Venter, H., Eloff, M., Labuschagne, L., Eloff, J. & von Solms, R.: *New Approaches for Security, Privacy and Trust in Complex Environments*. SEC 2007. IFIP International Federation for Information Processing. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-72367-9_12

Straub, D. W. (1990). Effective IS security: An empirical study. *Information systems research, 1*(3), 255-276. https://doi.org/10.1287/isre.1.3.255

Thamboo, J., Haraguchi, M., & Navaratnam, S. (2022). Resilience of critical infrastructure systems: A systematic literature review of measurement frameworks. *Infrastructures, 7*(5), 1-26. https://doi.org/10.3390/infrastructures7050067

Tundys, B. (2024). The Ripple effect-implications and consequences of incidental disruptions and black swan phenomena in the supply chain. *DIEM: Dubrovnik International Economic Meeting, 9*(1), 166-183. https://doi.org/10.17818/DIEM/2024/1.11

Trut, D. (2021). Aktualnosti zaštite kritičnih infrastruktura s naglaskom na javnu vodoopskrbu. *Police and Security 31*(2), 186 - 203. https://hrcak.srce.hr/en/clanak/407415

Wells, E., Boden, M., Tseylin, I. & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science, 15,* 1-15. https://doi.org/10.1016/j.pdisas.2022.100244

Yang, Z., Barroca, B., Mebarki, A., Laffréchine, K., Dolidon, H., & Lilas, L. (2024). Critical infrastructure resilience: A guide for building indicator systems based on a multi-criteria framework with a focus on implementable actions. *Natural Hazards and Earth System Sciences*, *24*, 3723–3753. https://doi.org/10.5194/nhess-24-3723-2024