European Research Studies Journal
Volume XXVIII, Issue 1, 2025

pp. 35-43

Critical Infrastructure Security in the Face of Contemporary Threats

Submitted 14/12/24, 1st revision 07/01/25, 2nd revision 25/01/25, accepted 15/02/25

Tadeusz Szczurek[1], Marzena Walkowiak[2]

Abstract:

Purpose: *The aim of the research, the conclusions of which are presented in this article, was to determine the position and role of Poland's critical infrastructure in the context of military and hybrid threats from the Russian Federation and Belarus.*
Design/Methodology/Approach: *The main research problem was formulated as the question: Which critical infrastructure systems are most significant given the dynamic changes in Poland's contemporary security environment? The research process employed both theoretical and empirical methods characteristic of the social sciences, including source analysis and diagnostic surveys (Wiśniewski). Data were collected through a survey of a representative sample of 395 individuals from across Poland. The study focused on the state's critical infrastructure systems—key services ensuring the population's security under contemporary threat conditions.*
Findings: *The research results indicate significant public interest in the issue of critical infrastructure protection in Poland. Respondents appreciated the importance of all sectors providing key services, with the highest indications observed in areas directly related to meeting basic existential needs, such as water, food, and energy systems and services. Respondents also rated the need to maintain effective rescue systems relatively high. According to the authors, this opinion may have been influenced by the ongoing war near Poland's eastern border. After several decades of peace in Europe, the Russian Federation's aggression against Ukraine has made the public aware that military threats remain real and that appropriate preparations are necessary.*
Practical Implications: *The practical implications primarily involve highlighting public expectations regarding critical infrastructure security for both central and local government administrations under conditions of hybrid actions and military threats from the Russian Federation.*
Originality/Value: *The research findings consider new challenges in the security environment of Central and Eastern Europe and may be applicable in other countries in the region.*
Keywords: *Security, threats, critical infrastructure, key services*

[1]*Prof. Dr. hab., Pomorska Szkoła Wyższa w Starogardzie Gdańskim, Poland,*
ORCID: 0000-0002-3433-8072, e-mail: tadeusz.szczurek@wat.edu.pl
[2]*Dr., Wojskowa Akademia Techniczna w Warszawie, Poland,*
ORCID 0000-0002-3317-562X , e-mail: marzena.walkowiak@wat.edu.pl

JEL Codes: *H56, K32, O33, Q34.*

Paper Type: *Research article.*

Acknowledgements: *The authors express their gratitude to all participants in the study.*

1. Introduction

The complex security situation in Central and Eastern Europe, including Poland, primarily stems from the ongoing war in Ukraine and hybrid attacks on the Belarusian-Polish border. The aggressive policies of the Russian Federation compel European Union member states to undertake specific measures to ensure the effective functioning of critical infrastructure systems.

Critical Infrastructure (CI) plays a key role in the security system of the modern state. It consists of selected elements of broadly understood state infrastructure, primarily with economic and social purposes, enabling the state to function normally. For facilities, devices, or installations to be classified as critical infrastructure, they must hold strategic importance for the functioning of the state economy.

In the process of qualifying specific facilities as critical infrastructure, it is worthwhile to refer to the perspective of crisis management experts who specialize in assessing whether a given facility (device, installation) can be considered part of the state's critical infrastructure. Experts focus less on the physical description of a given element and more on the services and functions provided by that element to society, aiming to assess the level of societal vulnerability to any disruptions in its operation.

The criteria used to determine the importance of the evaluated element (facility, installation, device, service) for the uninterrupted functioning of the broadly understood, comprehensive state infrastructure are divided into two types:

1. **Sectoral criteria** (systemic criteria) assigned to each CI system, covering the quantitative or functional parameters of objects, installations, devices, and services whose scope of operation may qualify them as critical infrastructure.
2. **Cross-sectional criteria**, qualifying elements as CI based on the consequences of their destruction or operational disruption and the impact of these consequences on the functionality of the state's overall infrastructure.

Elements (objects) are evaluated in cross-sectional reviews after being initially classified as critical infrastructure based on sectoral criteria.

These criteria are significantly influenced by changes in the security environment, which in recent years have been highly dynamic (Walkowiak, Szczurek).

2. Literature Review

In the literature and legal acts, the concept of critical infrastructure evolves alongside changes in the security environment, yet its essence remains ensuring the conditions for the functioning of the state and society in times of peace, crisis, and war (Tyagi *et al.*, 2023). In Poland and the European Union, critical infrastructure is defined as systems that ensure structural and personal security. However, recent years have witnessed a shift in some perspectives on critical infrastructure.

In Poland, the formal-legal definition of critical infrastructure remains as stated in the Crisis Management Act, describing systems that include facilities, devices, installations, and services essential for the security of the state and its citizens. This definition encompasses systems such as:

1. Energy supply, energy resources, and fuel;
2. Communications;
3. IT networks;
4. Financial systems;
5. Food supply;
6. Water supply;
7. Health protection;
8. Transportation;
9. Emergency services;
10. Continuity of public administration;
11. Production, storage, and transport of chemical and radioactive substances, including hazardous substance pipelines.

If any of these systems impact at least two member states of the EU, they are classified as European critical infrastructure (Ustawa).

The European Union particularly emphasizes services critical for maintaining essential social functions, economic activity, public health, safety, or environmental stability. This perspective on critical infrastructure is reflected in the European Parliament Directive. Sectors where key services are provided include:

1. Energy,
2. Transportation,
3. Banking,
4. Financial market infrastructure,

5. Health,
6. Drinking water,
7. Wastewater,
8. Digital infrastructure,
9. Public administration,
10. Space,
11. Food production, processing, and distribution (Dyrektywa).

The directive primarily addresses evolving hybrid and terrorist threats and the increased risk of natural disasters. It is crucial to consider dynamic changes in the security environment, including emerging threats such as the potential spread of the Russia-Ukraine conflict to EU states.

The implementation of EU law does not disrupt Poland's current view of critical infrastructure but expands its perception, particularly through the lens of its functionality. However, the core task for the administration remains unchanged: identifying all elements of critical infrastructure essential for the efficient functioning of the state and society.

Identifying dependencies between elements of critical infrastructure enables more precise assessment of the criticality of individual elements or even entire sectors. This facilitates the identification of the most critical infrastructures and the adoption of more cost-effective safety measures to reduce overall risk (Velinov *et al.*, 2023).

It should be noted that dependencies between infrastructures are often complex and not immediately apparent. These dependencies can lead to cascading disruptions or failures across various infrastructures, potentially significantly impacting multiple sectors, individuals, or countries (Setola and Theocharidou, 2016).

The issue of dependencies among infrastructures within EU member states is receiving increasing attention due to the progressing integration of numerous state functions within the community framework (Grima *et al.*, 2023).

3. Research Methodology

The empirical research primarily employed quantitative methods, while qualitative methods played a significant role in the selection of the research sample. A representative group of 395 individuals was selected. The sample was distributed based on age, gender, and place of residence (voivodeship). As a result, the study included 48% men and 52% women. By age, the percentage distribution was as follows:

- 18–20 years: 3%,
- 21–40 years: 33%,
- 41–50 years: 19%,

- 51–74 years: 36%,
- 75 years and older: 9%.

Qualitative selection ensured diversity in terms of place of residence, level, and type of education. The research group comprised:

- 19% rural residents,
- 24% residents of towns with up to 49,000 inhabitants,
- 17% from towns with 50,000–199,000 inhabitants,
- 21% from large cities (over 200,000 inhabitants).

Most respondents had higher education (46%). Secondary education was held by 42%, vocational by 10%, and only 3% had primary education. The group was dominated by individuals with technical education (40%), followed by humanities (21%), and economics (18%). Other groups included natural sciences (7%), medical (2%), artistic (2%), and other fields (10%).

Data for analysis were collected using a diagnostic survey method, specifically employing the CAWI technique. This method allowed respondents to express their opinions via an electronic questionnaire. Although the research was quantitative, the survey did not provide in-depth explanations of respondents' answers. It should be noted that such studies always carry the risk of false judgment or exaggeration.

The survey was conducted online. While internet usage has become widespread, it remains primarily the domain of younger generations. It can thus be cautiously assumed that older individuals were more likely to decline participation in the survey.

4. Research Results and Discussion

Perceptions of critical infrastructure within society are largely dependent on awareness of its role in ensuring security. Public sentiment may be shaped both by current needs and expectations related to the projected security environment.

In the research and subsequent analysis, factors influencing respondents' threat awareness were taken into account. The Russian-Ukrainian war has undoubtedly heightened awareness of Poland's military threat from the Russian Federation. Meanwhile, ongoing hybrid attacks and the influx of migrants from Belarus have revealed previously unconsidered threats to Polish society.

These are two of the most significant factors that may have influenced respondents' answers. Recognizing that not all respondents were fully familiar with the concept of critical infrastructure or key services, the question was preceded by a brief description of critical infrastructure. The task was stated as follows:

"Defined in the Crisis Management Act, critical infrastructure means systems and their functionally interconnected components, including buildings, devices, installations, and services essential for the security of the state and its citizens, as well as for the efficient functioning of public administration, institutions, and businesses. Please assign a score to the listed critical infrastructure systems (on a scale of 1–10, where 10 indicates the highest importance of the system)."

The responses, ranked from most important to least important based on respondents' evaluations, are presented in Table 1.

Table 1. *Summary of Responses Regarding the Importance of Critical Infrastructure Systems as Assessed by Respondents (On a scale of 1–10, where 10 represents the highest importance of the given system)*

Lp.	Critical Infrastructure Systems	Percentage of Respondents Assigning a Point Value to Each System on a Scale of 1–10									
		High Importance of Critical Infrastructure Systems			Medium Importance of Critical Infrastructure Systems				Low Importance of Critical Infrastructure Systems		
		10	9	8	7	6	5	4	3	2	1
		[%] (rounded to whole percentages)									
1.	Water supply	49	19	8	5	6	5	4	1	1	2
2.	Food supply	44	19	9	7	7	5	5	1	1	2
3.	Health protection	41	19	11	8	7	8	2	1	1	2
4.	Emergency services	40	22	9	7	7	7	2	1	2	3
5.	Communications	33	19	12	11	6	10	2	2	2	3
6.	Energy, energy resources, and fuel supply	34	15	13	12	6	12	2	1	2	3
7.	IT network systems	27	17	15	12	10	10	3	1	2	3
8.	Transportation	23	16	17	12	14	11	2	2	1	2
9.	Production, storage, handling, and use of chemical and radioactive substances, including hazardous substance pipelines	25	18	11	11	11	13	3	1	3	4
10.	Financial systems	18	16	14	14	13	13	4	2	2	4
11.	Systems ensuring the continuity of public administration	19	16	12	15	11	15	4	2	2	4

Source: *Own work.*

The data presented in the table clearly indicate the generally high assessment of the significance of critical infrastructure for the broadly understood security of the state and its citizens. For all systems within this infrastructure, the highest percentage of

respondents assigned a score of 10, representing the highest level of importance. Only a small percentage of respondents indicated low importance for these systems.

For the purposes of the scientific considerations outlined in this article, the research results were grouped as follows:

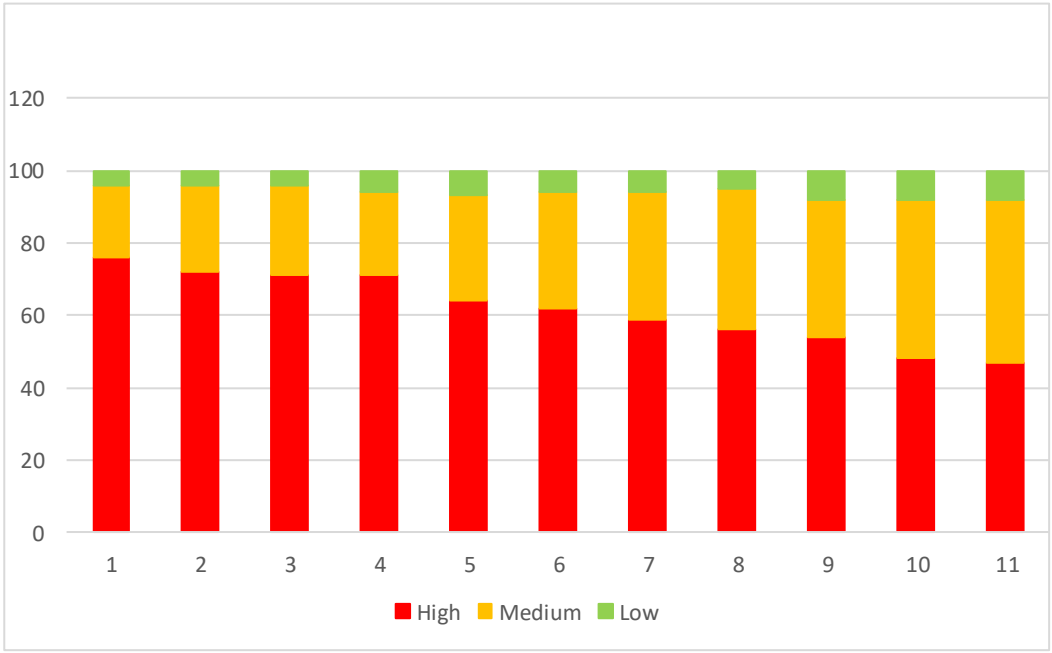
- **1–3 points** – considered as low importance for national security;
- **4–7 points** – considered as medium importance;
- **8–10 points** – considered as high importance.

After summing all responses within the above categories for each critical infrastructure system, the systems were ranked from the most important to the least important based on respondents' evaluations. In Table 1 and Figure 1, the most important system is marked with the number 1, and the least important system with the number 11. The ranking prepared based on this classification is as follows:

1. **Water supply systems** – rated highly by 76% of respondents, moderately by 20%, and as low by only 4%.
2. **Food supply systems** – rated highly by 72%, moderately by 24%, and as low by 4%.
3. **Health protection systems** – rated highly by 71%, moderately by 25%, and as low by 4%.
4. **Emergency systems** – rated highly by 71%, moderately by 23%, and as low by 6%.
5. **Communication systems** – rated highly by 64%, moderately by 29%, and as low by 7%.
6. **Energy, energy resources, and fuel supply systems** – rated highly by 62%, moderately by 32%, and as low by 6%.
7. **IT network systems** – rated highly by 59%, moderately by 35%, and as low by 6%.
8. **Transportation systems** – rated highly by 56%, moderately by 39%, and as low by 5%.
9. **Systems for the production, storage, handling, and use of chemical and radioactive substances, including hazardous substance pipelines** – rated highly by 54%, moderately by 38%, and as low by 8%.
10. **Financial systems** – rated highly by 48%, moderately by 44%, and as low by 8%.
11. **Systems ensuring the continuity of public administration** – rated highly by 47%, moderately by 45%, and as low by 8%.

The research reveals a consistent pattern: a large percentage of high ratings (47–76%) and a small percentage of low ratings (4–8%). The results of the assessments of the above systems (according to the numbering) are presented in Figure 1.

Figure 1. *The Importance of Critical Infrastructure Systems According to Respondents'Opinions.*



Source: *Own elaboration.*

The study revealed particularly high ratings for systems that have a direct impact on daily existence or are essential for survival. Hence, the highest scores were given to water and food supply systems, health protection systems, and emergency systems.

According to the authors of this article, the current political and military situation, particularly the full-scale war beyond Poland's eastern border, significantly influenced these assessments. While this cannot be stated with absolute certainty due to the absence of more detailed research allowing respondents to justify their choices, this hypothesis appears highly plausible.

5. Conclusions, Proposals, Recommendations

The approach to critical infrastructure evolves in parallel with emerging security challenges. Depending on the deficits identified in ensuring the population's basic conditions for existence and development, there is a need to focus efforts on maintaining the functionality and continuity of those systems requiring particular attention in a given situation.

Consequently, actions aimed at protecting European critical infrastructure following the military aggression against Ukraine on February 24, 2022, have primarily focused on energy supply systems, energy resources, and fuel.

This sector dominated EU-Russia relations before the introduction of economic sanctions against the Russian Federation, and it is precisely in this area that decisive actions were required to diversify supply chains. However, it is crucial not to overlook other sectors of critical infrastructure, as disruptions in the operation of any of them pose significant threats to national security. In the case of an EU member state, such disruptions often have implications for the security of other member states.

After welcoming a large wave of refugees from Ukraine, Polish society indirectly experienced the importance of ensuring basic services for a population affected by war. Direct or indirect reports from war-affected regions likely influenced the awareness of Polish society.

Concerns have emerged about the state's ability to meet the existential needs of its population in the event of war. These concerns directly translate into the perception of critical infrastructure, as it is this infrastructure that ensures the delivery of key services.

References:

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 roku, w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE, 27.12.2022, Dziennik Urzędowy Unii Europejskiej L 333/164 z dnia 27.12.2022.

Grima, S., Thalassinos, E., Cristea, M., Kadłubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital transformation, strategic resilience, cyber security and risk management. Emerald Publishing Limited.

Setola, R., Theocharidan, M. 2016. Modeling Dependencies Between Critical Infrastructures. In: R. Setola, V. Rosato, E. Kynakides, E. Rome (ed.), Managing the Compexity of Critical Infrastructures. A Modelling and Simulation Approach, Springer Open, p. 19. https://link.springer.com/book/10.1007/978-3-319-51043-9.

Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E., Thalassinos, E. (Eds.). 2023. Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy. Emerald Publishing Limited.

Velinov, E., Kadłubek, M., Thalassinos, E., Grima, S., Maditinos, D. 2023. Digital Transformation and Data Governance: Top Management Teams Perspectives. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (Vol. 111, pp. 147-158). Emerald Publishing Limited.

Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, Dz.U.2023.122, tekst jednolity.

Walkowiak, M., Szczurek, T. 2021. Critical infrastructure in view of the challenges to national security, Military University of Technology, Warsaw, 43-52.

Wiśniewski, B. 2020. Praktyczne aspekty badań bezpieczeństwa, Difin, Warszawa, 119-129.