Ivanov, E., & Georgieva, T. (2026). Resilience of critical infrastructure as a national security factor: Student perceptions of its performance in a current hybrid environment, *SCIENCE International journal, 5*(1), 133-139.
doi: 10.35120/sciencej0501133i UDK: 355.45:351.78[340.13(497.2)
355.4:004(497.2)
351.78:355.23(497.223)(047.31)

# RESILIENCE OF CRITICAL INFRASTRUCTURE AS A NATIONAL SECURITY FACTOR: STUDENT PERCEPTIONS OF ITS PERFORMANCE IN A CURRENT HYBRID ENVIRONMENT

*Elislav Ivanov[1*], Teodora Georgieva[1]*

[1]Rakovski National Defence College, Bulgaria, e-mail: e.ivanov@rndc.bg, t.georgieva@rndc.bg



**Abstract:** The contemporary hybrid security environment positions critical infrastructure as both a strategic asset and a potential vulnerability for national security. The growing interdependence among infrastructure sectors increases the risk of systemic disruptions with broad social and economic consequences. Evidence from recent armed conflicts, including the war in Ukraine, confirms the significance of infrastructure facilities as targets of combined and hybrid operations.

The aim of the present study is to assess the level of awareness among students at the Rakovski National Defence College regarding the resilience of critical infrastructure and its impact on national security. The research employs a qualitative design based on semi-structured questionnaires administered to a sample of 23 participants. The analysis focuses on determining the level of knowledge, the assessment of the condition and functioning of national infrastructure systems, as well as perceived risks and vulnerabilities.

The findings indicate a relatively high level of awareness concerning the strategic importance of infrastructure systems, while also identifying deficiencies related to resilience assessment and interinstitutional coordination. On this basis, recommendations are formulated to enhance education and professional training, and to strengthen the integrated civil-military approach to risk management. The resilience of critical infrastructure is conceptualized as a dynamic process requiring systematic prevention, protection, and recovery measures in the context of hybrid threats.

The results of the study indicate that Bulgaria's national critical infrastructure has clear regulatory frameworks and certain protective mechanisms in place, but practical effectiveness remains limited. The main challenges are related to the human factor, inter-agency coordination, preparedness, and vulnerability to hybrid and multi-domain threats. The international environment and regional conflicts significantly increase these risks. An integrated approach is required, including updating regulatory documents, enhancing technical and cyber protection, conducting regular exercises, facilitating information sharing, and promoting cross-sector cooperation, in order to ensure the resilience of critical infrastructure and the security of the state.

***Keywords:*** *critical infrastructure, resilience, national security, war in Ukraine.*

**Field:** Social sciences (security)

## 1. INTRODUCTION

Critical infrastructure is a set of systems and assets whose functioning constitutes a structural determinant of the functioning of society, the economy, and national security through its capacity to provide vital raw materials and services (Sertov, 2008). In its role as the foundation of state functioning, encompassing interrelated sectors, critical infrastructure represents an element of national security whose destruction leads to strategic vulnerability and reduced strategic autonomy (Flynn, 2004). Any attack against a specific sector may trigger systemic failure and cascading effects (Flynn, 2024) across the broader sphere of economic stability, governance, and societal well-being.

In this sense, the contemporary paradigm of interaction between critical infrastructure and national security is shifting from "asset protection" and sectoral protection toward the development of systemic resilience (Yossi Sheffi, 2013; Directive (EU) 2022/2557). A key concept describing reliability and continuous operation over time in the presence of vulnerabilities is resilience. The resilience of critical infrastructure is defined as the capacity to timely and effectively prevent, absorb, recover, adapt, and transform its core structures and functions in the face of threats, risks, and compromised security (UNDRR, 2022; NATO Strategic Concept, Madrid, 2022). Under conditions of interdependence and hybrid threats, critical infrastructure resilience becomes a central component of national strategy and a factor of deterrence (Nye, 2011). A state's ability to protect and restore its structures and functions enhances its strategic resilience and deterrence potential.

The conflict between Russia and Ukraine has affirmed and demonstrated its significance as a strategic instrument for achieving political and military objectives through humanitarian consequences for the population and the intensification of social tensions. The destruction of energy sector systems has

*Corresponding author: e.ivanov@rndc.bg

had a profound negative impact on civilians by depriving them of access to essential everyday resources necessary for survival.

The management of incidents of this type is gaining increasing importance not only at the tactical and operational levels but also at the strategic level, as it affects the long-term resilience of the state, the development of protective capabilities, and the ability to prevent and deter future threats. In this context, the war in Ukraine may be viewed as an infrastructural struggle for survival, in which the protection and resilience of critical infrastructure are decisive for the functioning of the state and its population under conditions of armed conflict (Ostrowski & Zych, 2024). Such a line of reasoning gives rise to the concept of "infrastructural warfare" or "war of attrition through systemic strikes," in which attacks against critical infrastructure are used as a means of disrupting state functioning and public services (Piekarski, 2025; Berezutskyi & Tokhtamysh, 2024).

## 2. MATERIALS AND METHODS

The present study examines the role of critical infrastructure as a strategic determinant of national security by analyzing the perceptions of students at the Bulgarian Military Academy. The empirical component covers a sample of 23 participants and is primarily based on a qualitative research design aimed at assessing the level of knowledge, degree of awareness, and expert judgment regarding the state and functioning of national critical infrastructure. A questionnaire consisting of 16 questions with open-ended response options was applied. Some questions also included a three-level quantitative scale -"Yes", "No", and "Partially". This publication presents and analyzes the responses to the items that the authors subjectively considered the most important.

*Empirical Study Design:*

Research Aim: to analyze students' perceptions of the resilience of national infrastructure as a factor of national security in the current hybrid environment.

*Research Objectives:*

1. To investigate the level of security culture among students through an analysis of their understanding of the essence, resilience, and determining factors of national critical infrastructure.

2. To assess the validity of students' evaluations of critical infrastructure resilience.

*Hypothesis 1:*

A higher level of awareness and understanding of the mechanisms that ensure the resilience of critical infrastructure is associated with a higher degree of established security culture.

*Rationale:*

The hypothesis is based on the theoretical relationship between awareness, risk perception, and the formation of a security culture. Knowledge of critical infrastructure resilience mechanisms—regulatory, organizational, technological, and operational—increases the ability to identify vulnerabilities, assess threats, and critically evaluate institutional readiness. Awareness functions as a cognitive prerequisite for developing resilient value attitudes and responsible behavior in the security domain. Therefore, a higher level of understanding of protective mechanisms correlates with a higher degree of established security culture (Schein, 2010).

*Hypothesis 2:*

The validity of students' evaluations of critical infrastructure resilience is negative.

*Rationale:*

Evidence indicates that Bulgarian critical infrastructure is outdated and inherited from the socialist period, and informed citizens recognize these structural weaknesses, leading to lower assessments of resilience. Frequent failures and incidents in water supply, energy, transport, and cybersecurity highlight insufficient risk management capacity. Greater knowledge fosters a critical security culture and recognition of real risks. While society often holds optimistic perceptions, awareness leads to a more critical evaluation of the current state. Thus, knowledge correlates with increased security culture and lower resilience assessments (Beck, 1992).

## 3. RESULTS

Below are the analyses of seven questions.

*1. State of Critical Infrastructure*

Critical infrastructure is defined as a structurally determining element of the national security system, directly, systematically, and proportionally influencing its functioning. Disruption of the functioning of facilities and elements of critical infrastructure creates an immediate threat to the life and

health of the population, including through the interruption of vital services and means of information and communication. The state of critical infrastructure is also considered a key factor for the effective command and control of elements of the national security system, particularly through communication and information networks. Disruption of these networks can lead to the disturbance of the planned functioning of security structures. Some respondents emphasize the strategic dimension of the issue, noting that the state of critical infrastructure can directly affect the sovereignty of the state, the capacity of the national economy, and the governability of state processes.

A comparison of EU and Bulgarian critical infrastructure reveals a perception of partial agreement dominance (57%), although a significant proportion of responses are positive (43%). Analysis of the open-ended responses shows that the linkage is sector-based. Elements of road infrastructure, the energy grid, healthcare systems, and information exchange between police and military structures are most often considered basic elements that function within broader European policies and mechanisms but are frequently subject to various national management and protection regimes.

*2. Vulnerability of Critical Infrastructure Facilities*

The vulnerability of critical infrastructure facilities is a key issue when considering it as a factor of national security. Respondents' perceptions outline a picture of complex and systemic vulnerability, in which interdependence between individual sectors amplifies the potential consequences of incidents. Particular concern is noted regarding the insufficient protection of the energy and transport sectors, including power transmission infrastructure, fuel and gas pipelines, and natural gas compressor stations. Airports, seaports, and main transport networks, as well as dams and dam walls, represent high risks to the population and the environment in the event of accidents or targeted impacts.

*3. Risk and Threat Prevention Measures for Critical Infrastructure*

Students identify a wide range of preventive measures aimed at mitigating risks and threats to critical infrastructure, covering strategic, operational, technological, and regulatory levels. At the strategic and defense level, air defense and missile defense (AD/MD) systems, monitoring and early warning systems, as well as aerial and technical surveillance capabilities, are highlighted.

At the operational and technological level, respondents emphasize the importance of advanced cybersecurity, integrated physical security systems—including video surveillance, sensors, and detectors—and the maintenance of rapid response teams. Limiting and controlling access to critical facilities is identified as a key preventive tool against sabotage and diversionary actions.

Significant emphasis is placed on intelligence and counterintelligence activities, including effective border control, gathering reliable information on planned impacts against critical infrastructure, and systematic monitoring of personnel across all agencies involved in its protection.

The importance of the regulatory and organizational framework is also noted, including the implementation of adequate prevention and protection plans, as well as the regular testing and evaluation of security systems through exercises and inspections. Respondents perceive the most effective protective measures as those that are integrated and function in synergy, rather than as isolated actions. The need to combine technical, organizational, and human components of security is emphasized.

*4. Effectiveness of the National Response System to Risks, Threats, and Incidents Targeting Critical Infrastructure*

Effectiveness is predominantly assessed negatively—responses indicating partial compliance dominate (61%), followed by clearly negative responses (30%). Affirmative responses confirming effectiveness account for only 9%.

The qualitative analysis of open-ended responses supports the trend observed in the quantitative assessments. The problems are differentiated across several areas: misalignment between the regulatory framework and its practical implementation, insufficient preparedness of personnel, weaknesses in interagency cooperation, alert systems, traffic management and control, as well as in the continuity and consistency of state administration in recent years. Some respondents expressed doubts regarding the ability to respond adequately to incidents affecting key energy facilities (substations, power transmission networks, thermal power plants) and critical healthcare institutions.

Although some opinions rated the level as "average" or providing "basic protection," the dominant perception is of limited, deteriorated, or insufficient readiness, as well as the absence of a comprehensive ("360-degree") protection model. Some respondents directly expressed distrust, rating capabilities as low or below expectations.

*5. High-Risk Means of Impacting Critical Infrastructure Facilities*

The criterion for classifying the highest-risk means of impacting critical infrastructure facilities is their potential to cause large-scale, long-lasting, and difficult-to-control consequences for the population, the environment, and state functioning. In this regard, weapons of mass destruction (nuclear, chemical,

and biological contamination) are highlighted, as well as kinetic impact means (conventional munitions, explosive devices, and improvised explosive devices), whose blast waves can cause serious destruction to infrastructure facilities. Cyberattacks and sabotage, which can disrupt management, coordination, and trust in institutions, are also noted, along with hybrid impacts, in which multiple elements or sectors of critical infrastructure are affected simultaneously, amplifying the cumulative effect and complicating response efforts.

*6. Hybrid Attacks as a Form of Threats to Critical Infrastructure*

Hybrid threats are perceived as among the most dangerous and impactful forms of direct threats to critical infrastructure facilities and systems due to their multi-domain, covert, and hard-to-detect nature. They exert strategic influence on the functioning of state institutions, the armed forces, and the national security system, with their primary role being the destabilization and erosion of state governance, social order, and public trust in institutions. By combining cyberattacks, diversionary actions, sabotage, and manipulation of public attitudes, hybrid attacks can overcome existing protective measures and distort objective reality. Significant emphasis is placed on the subversive nature of hybrid threats, which divert the attention of national security elements and decision-making bodies, thereby complicating timely and adequate responses.

*7. Influence of the International Environment on National Critical Infrastructure*

A clear consensus emerges regarding the direct impact of the international security environment on critical infrastructure, reflecting a high level of awareness of the interdependence between global security dynamics and the resilience of national critical infrastructure. Key factors identified include geopolitical instability, the expansion of regional conflicts, migration pressures, and the intensification of hybrid threats. Bulgaria's membership in NATO and the European Union is perceived both as a factor providing additional security guarantees and as increasing exposure to risks arising from allied commitments and geopolitical positioning.

The conflict in Ukraine is viewed as a catalyst for hybrid impacts, including cyberattacks, sabotage, and heightened intelligence activity, particularly in the context of the confrontation between Russia and Euro-Atlantic structures.

*1. Analysis of Students' Understanding of the Nature, Resilience, and Determining Factors of National Critical Infrastructure*

*Analysis of Results in Relation to Hypothesis 1*

Hypothesis 1 stated: A higher level of awareness and understanding of the mechanisms ensuring the resilience of critical infrastructure is associated with a higher degree of established security culture.

To evaluate the first hypothesis, two types of criteria were used: criteria for assessing awareness and criteria for assessing expertise.

Awareness includes: knowledge of the object or system (understanding of structural elements and functions), understanding of mechanisms (operation, vulnerabilities, protections, etc.), and understanding of interconnectedness (sectoral, transnational, strategic).

Criteria for assessing expertise relate to applied, practically grounded knowledge and the ability to analyze, evaluate, and make decisions. The main indicators are critical judgment and applied skills, systems thinking, forecasting abilities, and strategic planning.

The tables 1 and 2 below presented the number and content of semantic units supporting each of the criteria.

Table 1. Semantic Units from the Text Supporting the Criteria for Awareness

| Criterion | Semantic Units (Number) | Examples of Semantic Units |
|---|---|---|
| Cognitive Knowledge | 5 | "structurally determining element of the national security system," "impact on vital services," "impact on information and communication," "impact on sovereignty," "impact on the national economy" |
| Understanding of Mechanisms | 6 | "AD/MD systems," "monitoring and early warning systems," "advanced cybersecurity," "video surveillance, sensors, detectors," "rapid response teams," "prevention plans and exercises" |
| Understanding of Interconnectedness | 5 | "road infrastructure, energy grid, healthcare systems," "interagency cooperation," "transnational coordination," "EU and NATO frameworks," "European policies" |

Source: Authors' research

Table 2. Semantic Units from the Text Supporting the Criteria for Expertise

| Criterion | Semantic Units (Number) | Examples of Semantic Units |
|---|---|---|
| Critical Judgment and Applied Skills | 5 | "misalignment between regulatory framework and practice," "assessment of personnel," "interagency cooperation," "assessment of vulnerabilities in thermal power plants and substations," "assessment of transport hubs" |
| Systems Thinking | 5 | "interdependence between energy, transport, water supply, and healthcare," "complex consequences of incidents," "impact of hybrid effects," "strategic impact on state functioning," "influence on national security" |
| Forecasting Abilities and Strategic Planning | 4 | "updating the regulatory framework," "building specialized capabilities," "regular training and exercises," "anticipating hybrid and cumulative effects" |

Source: Authors' research

The results in the tables show that the students' open-ended responses contain numerous semantic units that directly correspond to the criteria for awareness (16 units) and expertise (14 units). The distribution of semantic units indicates that the text provides both a theoretical foundation (awareness) and practically oriented knowledge and skills (expertise), which supports the hypothesis that students who master the content and acquire objective knowledge develop a higher security culture. Therefore, the first hypothesis can be considered confirmed.

*2. Validity of Students' Evaluations of Critical Infrastructure Resilience***

*Analysis of Results in Relation to Hypothesis 2*

Hypothesis 2 stated: The validity of students' evaluations of critical infrastructure resilience is negative.

Table 3. Total Number and Examples of Semantic Units from the Text Supporting the Criteria for Awareness

| Criterion | Valence | Number of Semantic Units | Example Quotes from the Text |
|---|---|---|---|
| Awareness | Positive | 4 | "...high level of awareness of the interdependence between global security dynamics and the resilience of national critical infrastructure." |
| "Respondents perceive elements of road infrastructure, energy grid, healthcare systems..." | | | |
| Awareness | Negative | 9 | "...geopolitical instability, the expansion of regional conflicts, migration pressures..." |
| "Insufficient protection of the energy and transport sectors..." | | | |
| "Deficits in specific areas, such as water and underwater security..." | | | |
| Expertise | Positive | 6 | "...the need to combine technical, organizational, and human components of security." |
| "...updating the regulatory framework, building specialized capabilities, conducting regular training and exercises." | | | |
| "...integrated protective measures functioning in synergy." | | | |
| Expertise | Negative | 8 | "...respondents directly expressed distrust, rating capabilities as low..." |
| "...hybrid attacks can overcome existing protective measures..." | | | |
| "...complicating timely and adequate response by the national security system." | | | |

Source: Authors' research

The results in the table illustrate that the number of negative units (17) exceeds the positive ones (10), indicating that the validity of students' evaluations of critical infrastructure resilience is predominantly negative. The presence of numerous semantic units for awareness and expertise shows that their knowledge is objective and well-reasoned, not merely descriptive. The table supports Hypothesis 2.

## 4. DISCUSSIONS

Identifying students' perceptions of critical infrastructure in a context of hybrid challenges is valuable not only because of the demonstrated factual knowledge and analytical capabilities but also as an indicator of strategic culture, sensitivity to security issues, and a factor in political legitimacy and support for measures. According to Slovic (1987, pp. 280–285), perceptual assessments shape public pressure, political backing for measures, and the overall resilience of society. Similarly, Renn (2008, pp. 45–60) emphasizes that risk perception forms public attitudes and the willingness to support institutions and security measures, which is particularly significant in the context of hybrid and complex threats. Homer-Dixon (2006, pp. 45–52) postulates that if the future elite perceives critical infrastructure as vulnerable, this fact has direct implications for strategic planning, personnel effectiveness and motivation, as well as institutional legitimacy.

Respondents clearly identify hybrid threats as among the most dangerous for critical infrastructure due to their covert, multi-layered, and subversive nature. Their strategic impact on trust in institutions and state governability is emphasized. There is also a clear awareness of the interdependence between the international security environment and the resilience of national critical infrastructure. The war in Ukraine is perceived as a catalyst for hybrid impacts, including cyberattacks and sabotage, particularly in the context of the confrontation between Russia and Euro-Atlantic structures.

The demonstrated ability to strategically link the external environment with the state of internal infrastructure is a sign of a high level of analytical and professional maturity—a crucial element of security culture.

Empirical data confirm the existence of a paradoxical, yet logically grounded, effect: students with a deeper understanding of protective mechanisms identify more structural weaknesses. Awareness of the complex interdependence between sectors enhances the perception of systemic vulnerability. Knowledge of contemporary hybrid and cyber threats leads to a more critical assessment of national preparedness. Therefore, a lower evaluation of resilience is not an indicator of the absence of security culture; on the contrary, it reflects its presence at a higher level. These results can be explained through Ulrich Beck's concept of the "risk society": "Increasing awareness of systemic risks leads to greater criticality and caution in decision-making" (Beck, 1992, p. 22). High student awareness and expertise foster critical thinking and recognition of infrastructure vulnerabilities, which is a key component of security culture.

## 5. CONCLUSIONS

The approach to data analysis in the present report is based on a multidimensional methodological framework, in which specific specialized knowledge of critical infrastructure is used to derive indirect conclusions regarding students' trust in society, institutions, and security culture. Awareness and the level of expertise are considered both in their direct dimension—as indicators of cognitive levels of knowledge, understanding, and interpretation—and in a projective dimension, as a means of identifying deeper social attitudes, value orientations, and perceptions of institutional effectiveness. In this way, the analysis goes beyond a descriptive level and acquires an explanatory character, allowing the relationship between knowledge, evaluative positions, and trust in the national security system to be traced.

## ACKNOWLEDGEMENTS

The document was developed under the National Scientific Programme "Security and Defence", funded by the Ministry of Education and Science of the Republic of Bulgaria in implementation of the National Strategy for the Development of Scientific Research 2017-2030, adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

## REFERENCES

Batorowska, H. (2025). Information security awareness: Between ignorance and consciousness of threats. Polish Journal of Security and Threats, Article 1242. https://doi.org/10.36702/pb.1242

Beck, U. (1992). Risk society: Towards a new modernity (M. Ritter, Trans.). Sage Publications.

Berezutskyi, V., & Tokhtamysh, T. (2024). Risks of critical infrastructures during war. Law and innovative society, 2, 55-68, DOI:10.37772/2309-9275-2024-2(23)-5

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. (2022). Official Journal of the European Union. https://eur-lex.europa.eu

Flynn, S. E. (2004). America the vulnerable: How our government is failing to protect us from terrorism. HarperCollins Publishers.

Homer-Dixon, T. (2006). The Upside of Down: Catastrophe, Creativity, and the Renewal of Civilization. Island Press. (https://islandpress.org/books/upside-down)
Mantea, P. D. (2019). Security awareness in Romania: Security culture as a pillar of social responsibility development. Land Forces Academy Review, 24(3), 199–207. https://doi.org/10.2478/raft-2019-0023
NATO. (2022). NATO 2022 Strategic Concept. North Atlantic Treaty Organization. https://www.nato.int
Nye, J. S., Jr. (2011). The future of power. PublicAffairs.
Ostrowski, P., & Zych, R. (2024). State's resilience to critical infrastructure threats: The example of the Russian war on Ukraine. Teka Komisji Prawniczej PAN Oddział w Lublinie, 17(2), 349–363. https://doi.org/10.32084/tkp.9050
Piekarski, M. (2025). Critical infrastructure as a target of hybrid and conventional attacks: Lessons from the Ukrainian experience. Terrorism – Studies, Analyses, Prevention (special edition): 113–132.
Piotr Ostrowski & Radosław Zych (2024) – State's Resilience to Critical Infrastructure Threats: the Example of the Russian War on Ukraine. December 2024. Teka Komisji Prawniczej PAN Oddział w Lublinie 17(2):349-363. DOI:10.32084/tkp.9050
Principles for Resilient Infrastructure. (2022). UNDRR UN Office for Disaster Risk Reduction. Sendai Framework for Disaster Risk Reduction 2015-2030. 7bis Avenue de la Paix, CH1211 Geneva 2, Switzerland. https://www.undrr.org/publication/principles-resilient-infrastructure=
Renn, O. (2008). Risk Governance: Coping with Uncertainty in a Complex World. London: Earthscan.
Schein, E. H. (2010). Organizational culture and leadership (4th ed.). Jossey-Bass.
Sertov, P. (2008). Prevention as a primary method for protecting critical infrastructure in the work of the State Agency for National Security (DANS). In Proceedings of the Sixth International Conference "Security in Southeast Europe, Public–Private Partnership and Critical Infrastructure" (September 11–12, 2008). Academy of the Ministry of Interior.
Shahri, A. B., Ismail, Z., & Rahim, N. Z. A. (2013). Security culture and security awareness as the basic factors for security effectiveness in health information systems. Jurnal Teknologi (Sciences and Engineering), 64(2), 7–12. https://doi.org/10.11113/jt.v64.2212
Sheffi, Y. (2013). The resilient enterprise: Overcoming vulnerability for competitive advantage. MIT Press.
Slovic, P. (1987). Perception of risk. Science, 236(4799), 280–285. https://doi.org/10.1126/science.3563507
United Nations Office for Disaster Risk Reduction (UNDRR). (2022). Principles for resilient infrastructure. UNDRR. https://www.undrr.org/publication/principles-resilient-infrastructure