Dr. ***Tiana Kaleeva***
Expert at the Bulgarian Academy of Sciences (BAS)
Email: tianakaleeva@gmail.com

DOI: https://doi.org/10.37458/ssj.6.2.10
Review paper
Received: September 16, 2025
Accepted: December 1, 2025

ENHANCEMENT OF CRITICAL INFRASTRUCTURE RESILIENCE

Abstract: *The scope of this scientific article concerns the enhancement of the Resilience of strategic critical infrastructure facilities. The research emphasizes the crucial role of critical infrastructure and the necessity of adequate Resilience as part of its proactive protection approach. Risks and threats to critical infrastructure security are identified in three main categories (cybersecurity, human factors, and natural hazards). Based on the classification, opportunities for resilience enhancement are presented, along with recommendations for future improvements, with a primary focus on the physical and cyber security of critical infrastructure entities. The research is achieved through the application of documentary analysis and theoretical review, providing academic knowledge and practical solutions for the researched area.*

Keywords: *critical infrastructure resilience, cybersecurity, human factors, natural hazards, behavioral analysis*

1. INTRODUCTION

In contemporary times, critical infrastructure (CI) is not only an integral part of the modern world but also a rapidly evolving system with numerous elements, facilities, and fundamental operations. The emerging needs of today's societies displace traditional classifications. Besides the healthcare, telecommunications, transportation, and energy sectors, more recognizable are subsea cable systems, pipeline networks, utility water supply chains, electric power systems and substations, train rail networks, chemical storage facilities, etc. There are newly introduced CI elements related to start-ups, emerging technologies, and social needs, such as recently emerging cycling infrastructure, part of new green start-up activities regarding current ecological issues (Meijering, 2025).

Simultaneously with its growth, CI is facing further challenges, including an increasing trend of more sophisticated and large-scale malicious acts. That emphasizes the necessity of adequate facility protection, proactive security mechanisms, and enhanced Resilience. Based on that, the current article focuses on identifying and providing solutions for security enhancement through documentary analysis and theoretical review as a methodological approach.

2. CRITICAL INFRASTRUCTURE'S SIGNIFICANCE

The CI is identified as an element, facility, system, or part of it of significant importance, since its destruction or disruption causes negative consequences for the normal functioning of the system it is part of, as well as a substantial and continuous adverse effect. Consequently, this could result in severe facility damage, casualties, and financial and moral losses.

CI's essential services cover the energy, transportation, banking, healthcare, and public administration sectors, as well as the digital and space infrastructure divisions. CI are providing vital societal functions and financial activities (European Commission, 2023). Hence, the partial or total destruction of CI facilities affects the country's national defense and security, political and economic aspects of governance, social life, ecological factors, and the general loss of public trust.

Since critical entities consist of numerous facilities, often situated in more than one country or region, their effects are disseminated across several countries, underscoring the crucial importance of their protection. CI facilities are interconnected due to their multifunctional activities and responsibilities, making them interdependent – a security

incident in one facility would inevitably lead to a negative outcome in another, triggering a chain reaction among the existing CIs at the national, regional, or global level. Considering that, a legal framework focusing on the interconnected regulatory framework of CI is required. EU legislation provides examples in the field – the Directive on the Resilience of Critical Entities (strengthening Resilience against security threats) and the Network and Information Systems Directive (enhancing cybersecurity capabilities).

Although the focus on CI primarily centers on its functioning and application, it has substantial technological and financial impacts on development and maintenance, with greater emphasis on its protection. The size of the worldwide market for CI protection was estimated at USD 145.59 billion in 2024 and is expected to increase to USD 190.42 billion in 2030. The regional scope of the statistics includes North America, Europe, Asia Pacific, Latin America, the Middle East, and North Africa. North America is the largest market, while Asia Pacific is the fastest-growing (Market Analysis Report, 2023). These numbers underline the crucial importance of an adequate CI protection, high Resilience, and adaptability to security threats.

3. NECESSITY OF CRITICAL INFRASTRUCTURE RESILIENCE

Resilience is the capacity to anticipate and adjust to changing circumstances, and to endure and recover from disruptions caused by intentional hostile acts or natural disasters. Resilience plays a crucial role in sustainable development as it reduces the detrimental effects of unfavorable events on communities and maintains or enhances sustainable system performance (Linkov et al., 2014, p. 407). That is achieved through adjusting to significant changes caused by adverse events.

Infrastructure resilience depends on the Resilience of its critical subsystems. The ability of organizations that affect the operation and administration of infrastructure systems (suppliers, contractors, regulators, infrastructure operators and owners), as well as the systems' physical endurance, determines how resilient a particular infrastructure is. Organizational elements that affect infrastructure resilience include the presence of business continuity and contingency plans, the degree of professional competence, the frequency and capacity for testing plans, and the capacity for internal and external communication (Tretyakov, 2025).

Critical assets should be prioritized and evaluated to ensure proper protection of the involved infrastructures. The criticality assessment of infrastructure is essential for

introducing efficient protective measures to improve security in areas with a high level of disruption probability. A criterion limitation ought to be set in accordance with the magnitude of consequences arising from the destruction of a particular infrastructure. Several kinds of effects are considered regarding criticality, including the number of deaths, injuries to individuals, financial losses, reputational damage, etc. The decisive capabilities required to avoid, reduce, or compensate for failures that cause infrastructure issues are another way to define criticality (Gomes da Silva et al., 2025).

Resilience practices are based on three main core concepts (as shown in Figure 1) in relation to proactive and reactive approaches in overcoming security challenges: absorptive, adaptive, and transformative.

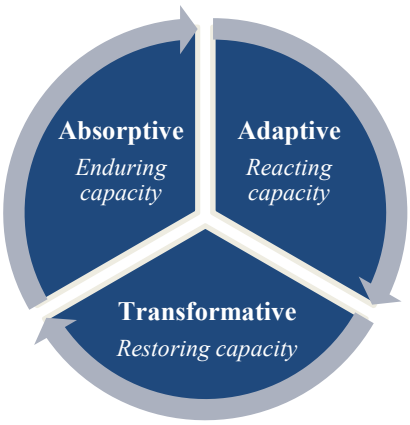

Figure 1. *Components of Resilience Capacity*

- ***Absorptive*** – represents an organization's capacity to endure a crisis while maintaining stability and preventive measures without experiencing a significant loss of functionality. To ensure stability and consistency of the processes, it incorporates governance mechanisms to withstand disruptive events and malicious acts (Kavanagh et al., 2025).

- ***Adaptive*** – signifies an organization's capacity to react and adapt to changing circumstances and prevent security failures. It includes adjustments to existing procedures and guidelines based on experience, aiming to improve current conditions.

- ***Transformative*** – outlines the organization's capacity to promptly restore functionality following disruptive incidents. It entails activities to reverse the consequences of disturbance and implement changes to mitigate future risks and threats (Tanner et al., 2017).

Resilience evaluation is considered a source of specifications for CI security development. In addition to solutions that suggest (such as constructing security systems), the organizational resilience assessment facilitates the identification of signs of emerging issues or opportunities for favorable change (Panevski, 2024, p. 1801). A comprehensive resilience strategy accounts for both known and unknown threats, providing a framework for evaluating and improving the Resilience of complex systems (Trump et al., 2025).

In recent years, CI has been dealing with a wide range of security challenges, testing its protection mechanisms and resilience endurance – malicious attacks towards industrial systems, energy companies, water systems, telecommunication and cloud infrastructures, gas operators, power grids, light-rail systems, water supply infrastructures, oil pipelines, etc. (ISTARI, 2024). The Nord Stream Incident in 2022 drew attention not only to the crucial role of gas pipelines as part of the CIs, but also to the disruptive effect of intentional sabotage. It results in multi-million-dollar financial losses and negative ecosystem and climate impacts (UN Environment Programme, 2025). A year before that, the Colonial Pipeline Attack caused widespread gasoline shortages and panic after a ransomware attack, underscoring the necessity of cybersecurity prioritization, particularly for critical facilities (Cybersecurity & Infrastructure Security Agency, 2023).

Cyberattacks represent an evolving threat worldwide. Adequate protection against cyberattacks has a significant impact on the economic, political, social, and defense aspects of national security. Disruptions to the regular operations of CI facilities are likely to cause additional risks, fatalities, and major crises at numerous systemic levels. Cyber risks are identified as a primary global risk for strategic infrastructures and critical facilities. Considering the shifting information landscape, ensuring adequate CI cyber protection is of utmost importance for national security (Kwilinski & Trushkina, 2024, p. 107). Developing cyber Resilience involves preparing for adverse consequences and adapting to them. It represents the system's capacity to withstand and recover from adverse cyber events (Sivwimi & Tembo, 2024, p. 51).

Resilience is also related to human factors. Low workforce capacity or hostile intent within an organization can lead to serious consequences for its infrastructure and operational effectiveness. Physical and cyber security of critical entities depend mainly on their personnel for the provision of protection, maintenance, and innovation, as well as for timely and adequate responses in cases of CI crises.

Resilience applies not only to intentionally caused disruptions and failures in CI with a hostile intent, but also to events related to **natural hazards**. Natural disasters like floods, earthquakes, storms, blizzards, wildfires, and tornadoes may impair critical facilities and trigger a domino effect across interrelated infrastructure. CI failures have a harmful impact on dependent people and societies (Pozo et al., 2025). The impact of natural hazards is becoming a significant concern, as climate-induced disasters are predicted to increase in the future (Dossi et al., 2025). Accident and emergency departments ought to be physically accessible at all times, particularly in emergencies. There is a direct interdependence among CIs related to disaster management, such as road and transportation networks, medical centers, fire stations, rescue departments, ambulance services, etc. (Moragues et al., 2023).

All that emphasizes the necessity of stable CI resilience, a high level of protection, and threat endurance. Efforts are to be distributed to protect the territory of CI and ensure safety for critical entities, facilities, personnel, consumers, third parties, and interrelated CIs.

4. OPPORTUNITIES FOR RESILIENCE ENHANCEMENT

Resilience enhancement should be performed in accordance with the particular CI's needs, based on identified risks and threats, previously and currently occurring vulnerabilities, level of preparedness, protection mechanisms, and endurance capabilities. Enhancement opportunities could be endorsed separately or simultaneously, depending on the desired outcome and security necessities. The article presents opportunities in four main areas: implementation of a governance framework; introduction of a cybersecurity framework; workforce capacity enhancement; and introduction of instruments for detecting hostile intent.

Implementation of a Governance Framework

A governance framework should reflect CI's unique organizational structure and business requirements. A practical governance framework improves financial performance, increases accountability and transparency, advances decision-making, and takes into account stakeholders' interests (Farnham, 2025). The following specifications are beneficial in framework establishment:

- Formulating the organization's ***goals and objectives*** in contribution to the mass public and other CIs' expectations;

- Identifying ***types of critical services*** and systems, along with the ***number of CI facilities involved***, their responsible entities, personnel, and anticipated results;
- Establishing a ***governance structure***, including hierarchy level, escalation duties, ethical code, board performance evaluation, and internal risk management;
- Defining workforce capacity and ***specific personnel competences*** needed, setting a plan for subsequent training and skills enhancement;
- Outlining in advance ***challenges and opportunities*** based on previous experience and expected future fluctuations;
- Determining the type and number of ***end-users and communities***, based on their needs;
- Adopting a ***crisis management procedure*** based on identification, prevention, reaction and transformation approaches;
- Setting ***security protocols and regulations*** in Compliance to the legal legislation, security standards, requirements and instructions on the organizational, national and regional level.

Nevertheless, potential difficulties should also be taken into consideration when developing a governance framework, such as coordination challenges, ethical concerns, unforeseen legal complications, insufficient voting procedures and decision-making processes, dysfunctional hierarchical structure, unwillingness to accept and implement organizational and administrative changes, etc.

Introduction of a Cybersecurity Framework

An appropriate cybersecurity framework is considered a fundamental element in establishing stable cybersecurity and adequate CI protection, both digitally and physically. Since CI resilience is increasingly tied to countering cyber threats, implementing an appropriate framework is a crucial element of cybersecurity. Its components (illustrated in Figure 2) aim to overcome specific cyber challenges and to develop safeguards against cyber threats and vulnerabilities (Alozie & Chinwe, 2025, p. 562).

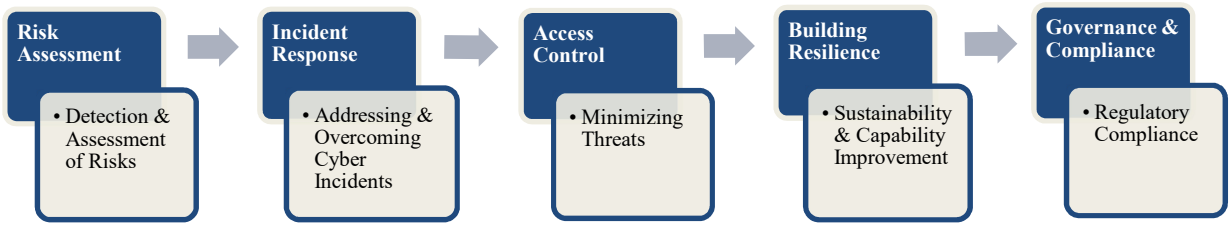

Figure 2. *Components of Cybersecurity Framework*

The framework should provide comprehensive, structural mechanisms for cybersecurity, aligned with existing operational policies and regulatory requirements, to ensure adaptability and stability. Its elements regard the following activities:

- ***Risk Assessment*** – focuses on detecting, assessing, categorizing, and ranking CI risks and threats, including those of a cyber nature. It enables the evaluation of the likelihood of threats emerging and their negative impact on CI entities.
- ***Incident Response*** – creates both proactive and reactive tools for identifying, addressing, and resolving cybersecurity incidents. It includes performance of root cause analysis, escalation protocols, incident response and recovery plans;
- ***Access Control*** – emphasizes preventing unauthorized access, minimizing insider threats, and reducing coercion of security responsible personnel. Access control may be achieved through numerous confirmation techniques – multi-factor authentication, device verification based on roles and responsibilities, Compliance with access escalation and regular performance of cybersecurity audits.
- ***Building Resilience*** – guarantees ongoing functioning and operational capabilities of CI during and after cyber incidents and deliberate attacks. The process involves the implementation of strategies to sustain operations during disruptions and mitigate potential failures, as well as performing regular incident recovery exercises to maintain organizational preparedness.
- ***Governance and Compliance*** – ensures cybersecurity practices conform to the set requirements and governance guidelines. Essential is the conduct of regular compliance assessments that align with the organizational structure and predefined policies.

Workforce Capacity Enhancement

CI resilience relies extensively on human factors. Workforce capability is crucial for the effective daily operations and business processes. Considering that, the following components (workforce resilience, cross-sector collaboration, and community engagement) are introduced with a focus on their essential roles:

- ***Workforce resilience*** – crucial for ensuring effective recovery capabilities. By encouraging a resilient culture, organizations train their personnel to manage exposure to prolonged stress and operational interruptions while maintaining high performance during business-as-usual and crisis events.

- ***Cross-sector collaboration*** – achieving collaboration among different CI is vital for the fulfilment of a cohesive and efficient recovery, maintaining a high level of security and managing the aftermath of disruptions or destruction of the infrastructure. Nevertheless, miscommunication, conflicting priorities, and bureaucratic issues are common challenges that obstruct cooperative efforts. Alliance between organizations and across interrelated sectors is fundamental to the effective recovery of the CI within.
- ***Community engagement*** – enhancing the capacity for engaging with the community and stakeholders improves the efficiency of the recovery efforts. The manner in which communities interact with affected communities can impact the recovery process, both positively and negatively, underscoring its essential role in minimizing disruption and increasing community satisfaction (Wills & Pemberton, 2025).

Instruments for Detection of Hostile Intent

Hostile intent is related to malicious acts directed at a particular organization, its facilities, processes, services, personnel, or customers. It might include acts of aggression and terrorist attacks with short- or long-term negative impact on CIs. As an instrument for early detection of malicious intent with the potential to prevent and protect CIs, behavioral analysis (BA) is a valuable tool for identifying suspicious, criminal, or hostile behavior. The development of various programs and surveillance systems would facilitate the prevention of crime (including terrorist attacks). They also provide control over aggression in various crowded facilities, such as CIs of strategic importance.

In general, BA programs have a specific basic structure (shown in Figure 3). It begins with an assigned team of experts (IT specialists, BA and security experts, etc.). They are responsible for building the program, based on their professional experience and competencies. A functioning program **algorithm** is developed, along with the leading behavioral indicators considered and predefined evaluation mechanisms—for example, 20 suspicious behavioral traits for monitoring and detection in individuals.

After the program is created, it initiates **monitoring and analysis of subjects** in the territory of CI's entities. Depending on previously identified vulnerabilities and threats to the particular infrastructure and the set desirable goals, it is positioned so that the examined subjects are unaware they are being monitored and analyzed.

It is mandatory to define **eligibility criteria** to be considered during the monitoring process. For example, up to 8 of 20 behavioral indicators displayed by an individual are acceptable. If eight or more suspicious individuals are present, the program must notify

security officers. They are separated and subjected to additional screening to determine whether they are hostile.

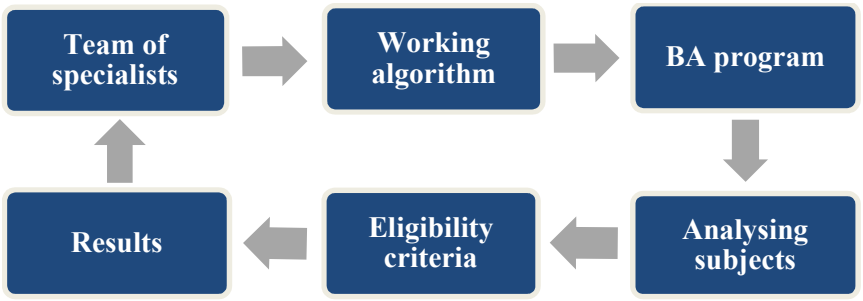

Figure 3. *Structure of Behavioral Analysis Program*

Potential challenges regarding BA programs should be considered as well:

- BA programs ought to be as ***gender- and race-neutral*** as possible. Hence, at the beginning and end of the process, the human factor is assigned to make the final decisions about the program's scope, algorithm, eligibility criteria, and to determine suspicious behavior and detect hostile individuals. In addition, the programs should protect individuals' ***personal data***, since BA mainly monitors, examines and analyzes various biometric data;
- An effective BA program is ***developed in accordance with the specific critical facility's needs***. It should be designed to meet the precise threats and risks of the given CI. Creating a universal program that would apply to mass requirements in multiple entities and in different territories is an unrealistic initiative, since it is not possible to unify the needs and threats of these critical entities.
- The introduction of a BA program in CI's security systems is a ***significant financial investment*** that should be assessed and justified in advance. As a strategic planning process, this requires continuous coordination and management approval (Gechkova, 2025, p. 68). In the BA program implementation, the initial investment must be rationally subsidized through own or borrowed funds, along with a plan for financial assessment and expected future return.

5. RECOMMENDATIONS FOR FUTURE IMPROVEMENTS

Based on previously presented opportunities for enhancing CI resilience, the following recommendations are made:

- ***Encouraging a better understanding of delinquency and its*** negative impact on CI functioning and security systems. A deeper understanding can assist governing bodies in determining adequate reporting thresholds, categorizing security events by their magnitude, and defining approved roles and responsibilities shared between government and industry

stakeholders. That approach aimed to facilitate national preparedness and crisis management in times of emergencies and conflicts, as well as to provide guidelines for appropriate investment actions (Kavanagh et al., 2025).

- ***Updating the related legal framework*** to reflect on the infrastructure's criticality adequately, appropriate legal actions, and regulatory background for CI protection;
- Outlining pathways for ***new security standards adoption*** and abolition of outdated ones;
- Establishing ***instruments against hostile intents*** and a ***timely response*** to malicious acts as a proactive approach for improving security and safety on the territory of CI facilities;
- ***Aligning regulations*** among related countries or regions, aiming at better cooperation and synergy;
- Focusing on national security and Resilience, as well as the establishment of ***response management*** and ***crisis preparedness plans***;
- ***Investing in*** maintenance and ***innovation*** activities concerning CI protection and a high level of security;
- Developing mechanisms for ***reporting and classifying security incidents*** in an adequate and timely manner, along with the respective undertaken actions, outcomes and responsible persons involved;
- Increasing ***personnel preparedness*** for response to CI attacks and disruptions. It could be achieved by addressing gaps in workforce resilience, inefficient cross-sector collaboration, and insufficient community engagement.
- ***Overcoming cybersecurity vulnerabilities and threats*** through implementation of a cybersecurity framework based on risk assessment, incident response, access control, building Resilience, governance and Compliance;
- Paying attention not only to ***cyber risks*** but also to those arising from ***hostile intent***, ***natural hazards*** and ***malfunctioning disruptions***, etc.

6. CONCLUSION

CI's significance to national and regional security underscores the need for proper protection, stability, and Resilience against security vulnerabilities and threats. Appropriate mechanisms for resilience improvement could be applied regarding cyber-attacks, malicious

acts and natural hazards. The introduction of a governance framework, a cybersecurity framework, BA programs, and workforce capacity enhancement is favorable for future resilience improvement and CI protection. Constant exploration of resilient measures and approaches is beneficial not only to the CI maintenance but also to its safety.

REFERENCES

1. Alozie, C. E. & Chinwe, E. E. (2025). Developing a Cybersecurity Framework for Protecting Critical Infrastructure in Organizations. Iconic Research and Engineering Journals, 8(7). 562-576. [Online]: https://doi.org/10.5281/zenodo.14740463.
2. Cybersecurity & Infrastructure Security Agency. (2023). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. [Online]: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.
3. Dossi, S. et al. (2025). Wildfire Risk-Reduction Guidance for European Critical Infrastructure: Case Study of an Electrical Substation in Austria. EGU25-10265. EGU25. Copernicus Meetings. [Online]: https://doi.org/10.5194/egusphere-egu25-10265.
4. European Commission. (2023). Critical Entities' Resilience. [Online]: https://ec.europa.eu/commission/presscorner/detail/sk/ip_23_3992.
5. Farnham, K. (2025). What Is a Governance Framework?. Diligent. [Online]: https://www.diligent.com/resources/blog/what-is-governance-framework.
6. Gechkova, T. (2017). The Prioritization of the Measures for the Protection of the National Critical Infrastructure (Strategic Emphases). Economic Alternatives, 31(2). 68-76. [Online]: https://www.unwe.bg/alternativi/bg/journalissues/article/11099.
7. ISTARI. (2024). Analysis of Top 11 Cyber Attacks on Critical Infrastructure. [Online]: https://istari-global.com/insights/spotlight/analysis-of-top-11-cyber-attacks-on-critical-infrastructure/.
8. Kavanagh, C. et al. (2025). Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure. UNIDIR. [Online]: https://unidir.org/publication/achieving-depth-subsea-telecommunications-cables-as-critical-infrastructure/.
9. Kwilinski, A. & Trushkina, N. (2024). Impact of Cyber Risks and Threats on the Critical Infrastructure Development: Visualization of Scientific Research. Proceedings of the International Conference on Applied Innovations in IT, 2. 107-119. [Online]: https://doi.org/10.25673/118123.
10. Linkov, I. et al. (2014). Changing the Resilience Paradigm. Nature Climate Change, 4. 407-409. [Online]: https://doi.org/10.1038/nclimate2227.

11. Market Analysis Report. (2023). Critical Infrastructure Protection Market Size Report, 2030. [Online]: https://www.grandviewresearch.com/industry-analysis/critical-infrastructure-protection-cip-market.
12. Meijering, B. (2025). Cycling as Critical Infrastructure for Green Start-Ups: A Multilevel Analysis in Germany. Sustainability, 17(8). [Online]: https://doi.org/10.3390/su17083441.
13. Moragues, A. et al. (2023). Analysis of Road Accessibility by Residents and Tourists to Public Hospitals in Mallorca (Balearic Islands, Spain). Sustainability, 15(10). [Online]: https://doi.org/10.3390/su15108182.
14. Panevski, V. (2024). Critical Infrastructure Resilience Assessment as a Source of Requirements for the Security Systems Development. Proceedings of the Bulgarian Academy of Sciences, 77(12). 1801-1807. [Online]: https://doi.org/10.7546/CRABS.2024.12.08.
15. Pozo, A. M. M. et al. (2025). Measuring Spatial Accessibility to Critical Infrastructure: The Access Road Identification Model. International Journal of Critical Infrastructure Protection, 49. [Online]: https://doi.org/10.1016/j.ijcip.2025.100760.
16. Silva, E. G. et al. (2025). International Perspectives on Critical Infrastructure: Evaluation Criteria and Definitions. International Journal of Critical Infrastructure Protection, 49. [Online]: https://doi.org/10.1016/j.ijcip.2025.100761.
17. Sivwimi, G. & Tembo, S. (2024). Evaluation of a Cyber Security Resilience as a Factor for Regulating Critical Infrastructure. Computer Science and Engineering, 14(3). 51-55. [Online]: https://doi.org/10.5923/j.computer.20241403.01.
18. Tanner, T. et al. (2017). Challenges for Resilience Policy and Practice. Working paper, 519. [Online]: https://doi.org/10.13140/RG.2.2.30130.30402.
19. Tretyakov, O. et al. (2025). Methodology for Quantitative Assessment of Critical Infrastructure Resilience. Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks. [Online]: https://shorturl.at/K3tJs.
20. Trump, B. et al. Threat-Agnostic Resilience: Framing and Application for Critical Infrastructure. [Online]: https://doi.org/10.48550/arXiv.2501.01318.
21. UN environment programme. (2025). Pipeline Blasts Released Record-shattering Amount of Methane: UNEP Study. [Online]: https://shorturl.at/uqvIm.

22. Wills, J. & Pemberton, J. (2025). The Human Element in Critical Infrastructure: Strengthening Workforce Preparedness for Restoration and Resumption After Mass Disruption. Institute of Homeland Security. [Online]: https://hdl.handle.net/20.500.11875/5067.