European Research Studies Journal
Volume XXVIII, Issue 2, 2025

pp. 610-621

Critical Infrastructure Security Management in the Era of Cyber Threats

Submitted 14/04/25, 1st revision 10/05/25, 2nd revision 24/05/25, accepted 20/06/25

Marta Chodyka[1], Sławomir Żurawski[2], Sylwia Wojciechowska-Filipek[3], Zbigniew Ciekanowski[4], Sławomir Mazur[5]

Abstract:

Purpose: *This article analyses contemporary cyber threats against critical infrastructure and identifies effective strategies for managing its security under conditions of increasing digitisation. The study focuses on assessing the impact of attacks on the energy, transportation, water supply, and healthcare sectors and identifying institutional and legislative measures to strengthen the resilience of these systems.*

Research Methodology/Approach: *The paper uses theoretical methods, including literature analysis, cybersecurity industry reports and case studies of selected incidents that affected critical infrastructure in 2023-2025. The first part characterises the main types of cyber attacks (ransomware, DDoS, APT) and the sectors most vulnerable to disruption. This follows an analysis of the consequences of selected attacks on state and private infrastructure operations. The final section presents a systemic approach to security management, including the concepts of resilience, redundancy, business continuity and legislative solutions such as the NIS2 directive and national infrastructure protection programs. The research problem was formulated: What cyber threats pose the most significant challenge to critical infrastructure security, and what strategies can ensure adequate protection? The hypothesis is that effective protection of critical infrastructure requires integrated actions based on technology, regulation and cross-sector and international coordination.*

Results: *The conclusions of the analysis indicate that critical infrastructure remains one of the most common targets of cyberattacks, and their effects are often cascading and cross-border. Protecting these assets requires a systems approach that combines threat detection technologies, business continuity planning, collaboration between operators and security services, and regulatory alignment with the dynamically changing threat landscape.*

Practical implications: *The findings are essential for state security institutions, critical service operators and policymakers. Adequate infrastructure protection requires technological investment and awareness-building among management and operational staff,*

[1] *John Paul II University in Biala Podlaska, ORCID:0000-0002-8819-2451, e-mail: ....*

[2] *Andrzej Frycz Modrzewski University in Krakow, ORCID: 0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl;*

[3] *……………………….ORCID: 0000-0002-1847-1957, e-mail: wojciecs@wit.edu.pl;*

[4] *War Studies University, ORCID: 0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl;*

[5] *The same as in 2, ORCID: 0000-0002-5056-2280, e-mail: smazur@orange.pl;*

as well as regular training, resilience testing and security audits. Lessons can be used in the design of public policies and the development of crisis management plans.

Originality/Value: *The article brings value by comprehensively addressing the problem of critical infrastructure security management in the context of growing cyber threats. It combines technological, institutional and legal analysis to formulate practical recommendations for national and international protection systems. It emphasises the need to strengthen cross-border cooperation and harmonise protection standards within structures such as the European Union and NATO.*

Keywords: *Critical infrastructure, security management, cyber threats.*

JEL: *M15, Q48.*

Paper type: *Research article.*

1. Introduction

Modern societies increasingly rely on technical and ICT systems, the uninterrupted operation of which is the foundation of national, economic and social security. In this context, critical infrastructure - understood as a set of facilities, equipment and services that are key to the functioning of the state and the protection of citizens' lives - acquires special importance. The development of digital technologies, while bringing tangible operational and economic benefits, simultaneously exposes critical infrastructure to new and complex threats, primarily in the cyber dimension.

Cyber attacks on energy, water, transportation or financial systems are becoming increasingly sophisticated, and their effects can be comparable to the consequences of traditional physical attacks. In an era of information warfare, increased activity by hacking groups and rising incidents of ransomware, managing the security of critical infrastructure requires not only technological preparedness but also a strategic approach based on risk analysis, systems resilience and multifaceted cross-sector cooperation.

This article highlights current challenges and best practices in critical infrastructure security management in the context of cyber threats. It analyses normative and institutional aspects and technical and organisational protection mechanisms. Special attention is paid to the role of the state, infrastructure operators, and cybersecurity services in building systemic resilience to 21st-century threats.

2. Importance of Critical Infrastructure Under Modern Threats

Critical infrastructure plays a key role in ensuring the continuity of the functioning of the state, the economy and the daily lives of citizens (Ciekanowski, Żurawski, and

Wyrębek, 2023, p. 266). According to the definition adopted in the Polish legal system, as well as in international documents (e.g., European Union directives), critical infrastructure is systems, facilities and installations, the destruction or disruption of which would result in a serious threat to national security, human health, public order or basic economic functions (Crisis Management Act of April 26, 2007, Article 3).

Critical infrastructure classification includes energy, water and food supply, transportation, communications, health care, finance, public administration, and emergency and defence services. It should not be forgotten that some of this infrastructure is in private hands (communications, ICT systems, transportation) (Milewski, 2016, p. 101).

The National Program for Critical Infrastructure in Poland presents criteria for identifying CI. The requirements are divided into two groups:

1) system criteria - characterising quantitatively or subjectively the parameters (functions) of an object, device, installation or service, the fulfilment of which may cause inclusion in the critical infrastructure.

2) cross-cutting criteria - describing parameters relating to the consequences of the destruction or cessation of operation of an object, device, installation or service. Cross-cutting criteria include:

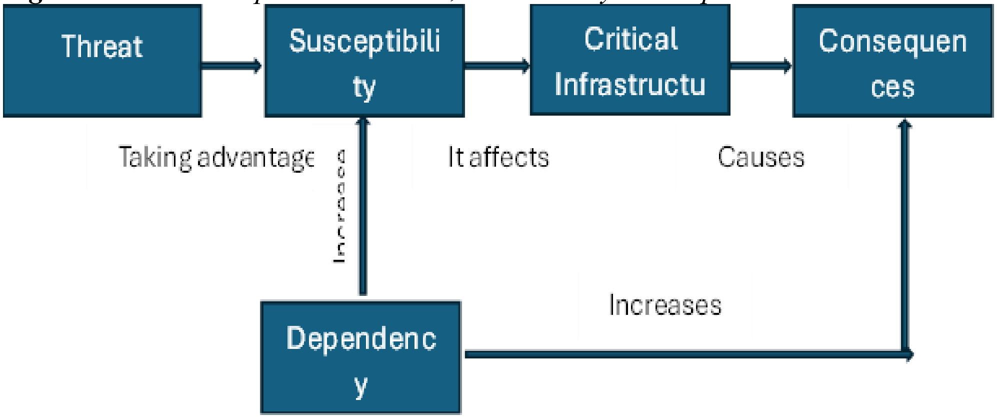
- human casualties,
- financial impact,
- the need for evacuation,
- loss of service,
- recovery time,
- international effect,
- uniqueness (National Critical Infrastructure Program, 2023, p. 13).

Modern societies are increasingly dependent on information and communications technology (ICT), which has been integrated into the operation of critical infrastructure at almost every operational level. Air traffic management systems, power grids, transmission buses, banking servers, and hospitals rely on ICT infrastructure, the integrity and availability of which are prerequisites for systemic stability (Thalassinos *et al.,* 2023).

As a result, digitisation, a vehicle for innovation and efficiency, has also become a source of new threats of an asymmetric nature, especially in cybersecurity. Accordingly, technological development creates a system of interdependence and interaction between the state and infrastructure (Pyznar and Abgarowicz, 2014, p. 25). Critical infrastructure is highly vulnerable to cyberattacks (Dynes, Goetz, and Freeman, 2010, p. 15; Grima *et al.,* 2025; 2024; 2023; Velinov *et al.,* 2023). Critical infrastructure's vulnerability to cyberattacks stems not only from its technical complexity but also from the fact that many of its components operate as part of distributed systems, often managed by different entities and vulnerable to vulnerabilities, both in the technical and organisational realms.

Today's cyber attacks increasingly exploit automated penetration techniques, social engineering, and vulnerabilities in outdated SCADA systems or Internet of Things (IoT) devices, making critical infrastructure particularly vulnerable to cascading disruptions. Disruption of one part of the infrastructure - such as the energy system - can result in the paralysis of subsequent sectors, including health care, transportation, supply chains and public policy. The diagram below shows the relationship between threat, vulnerability and impact.

Figure 1. *Relationship between threat, vulnerability and impact.*



Source: *National Critical Infrastructure Program, 2023, p. 29.*

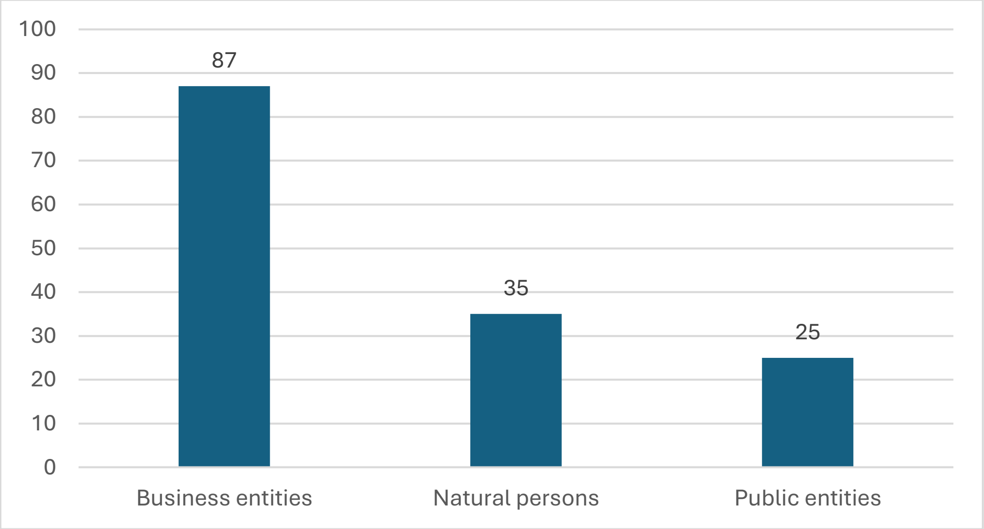
From a security perspective, critical infrastructure is a strategic asset that must be protected from physical threats and cyber disruptions. In an era of hybrid aggression and escalating actions by non-state and state actors, critical infrastructure protection requires a new approach that integrates risk management, systems resilience and real-time incident preparedness. Critical infrastructure is undoubtedly very important for the proper functioning of any institution, and the facilities and systems that comprise it are crucial from a security perspective (Wódkiewicz, 2022, p. 157).

3. Cyber Threats to Critical Infrastructure and Risk Analysis

In the era of digitisation, critical infrastructure is becoming increasingly vulnerable to cyber activities, sabotage and cyber attacks inspired by hostile states and non-state actors. Hazardous attacks are targeted using advanced hacking techniques to paralyse key sectors of public and economic life. Characteristic of modern threats are: ransomware attacks, leading to data encryption and extortion; DDoS attacks, aimed at overloading network services and crippling systems; and actions from the

APT (Advanced Persistent Threat) category, which involve long-term covert penetration of systems to steal data, sabotage or prepare the ground for a future attack (Ciekanowski *et al.,* 2023, p. 790). Figure 2 below shows incidents related to ransomware malware attacks.

Figure 2. *Number of incidents related to ransomware malware attacks in 2024.*



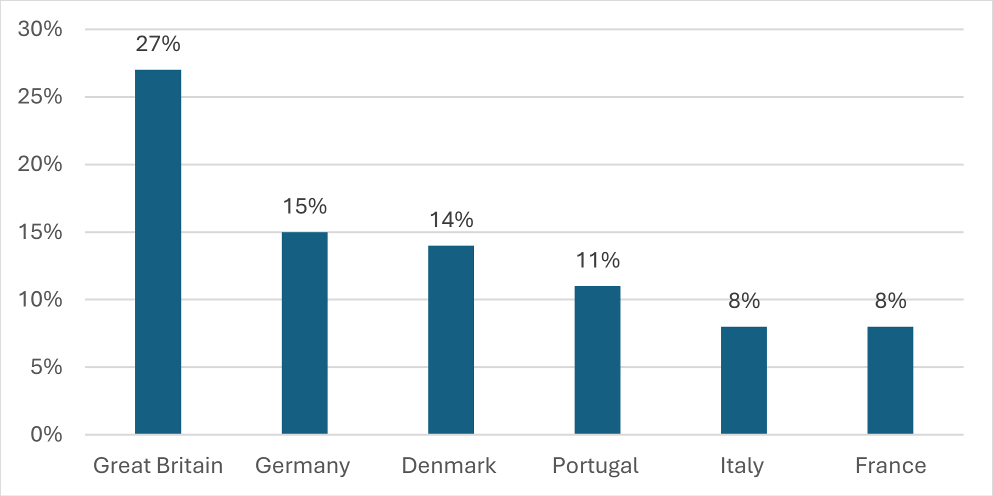
Source: *CERT Polska Activity Report for 2024.*

In 2024, CERT Polska recorded 147 incidents related to ransomware attacks. This is a decrease of about 8% from the record year 2023 (CERT Polska Report, 2024). In 2024, there was again increased activity by advanced APT groups operating on behalf of foreign countries. Their operations were mainly of an espionage and disinformation nature.

The predominant forms of attacks were acquiring login credentials for e-mail accounts, the distribution of malware, and interference with industrial systems. Unlike in earlier years, cybercriminals' activities were no longer limited to large corporations and public institutions - smaller companies relevant to the supply chain were also attacked, and even people in the immediate circle of the original targets, such as their relatives or acquaintances (CERT Poland Report, 2024).

In recent years, critical infrastructure has increasingly become the target of advanced cyberattacks. According to data from the European Cyber Incident Repository, about 1,400 such incidents were registered in 2023-2024, with more than half involving this key segment. Health systems, financial institutions, and the telecommunications, transportation, and energy industries have proved to be the most vulnerable (https://eurepoc.eu). In 2023, Europe was the target of 32% of global cyberattacks. The chart below shows the countries that were most attacked.

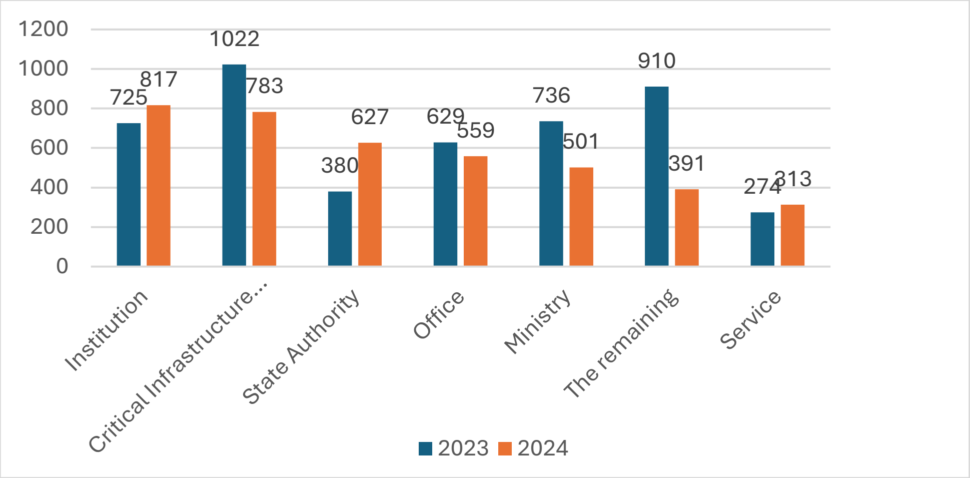
Figure 3. *Most frequently attacked countries by cyberattacks.*



Source: *X-Force Threat Intelligence Index, Institute for Business Value.*

The situation in 2024 was even more alarming. Some 500 suspicious incidents were reported in Europe, one in five linked to Russian hybrid attacks or espionage activities. The situation in Poland is also worth noting. Considering the breakdown of incidents by sector, it should be pointed out that in 2024, according to the CISIRT report, the most significant number of incidents, as in 2023, were in the Institutions sector and just Critical Infrastructure Operators. Below is the number of incidents reported by national cybersecurity system entities in 2023 and 2024 by industry.

Figure 4. *Number of incidents reported by national cybersecurity system entities in 2023 and 2024 by sector.*



Source: *Report on Poland's cybersecurity in 2023 and 2024.*

Even more worrisome is that data breaches are often just the beginning of larger and more coordinated campaigns. Cybercriminals are openly trading exploits on the dark web to attack critical infrastructure such as power grids, health networks and industrial systems.

Examples of incidents in recent years show the scale and impact of cyber threats against critical infrastructure. In 2007, a series of cyberattacks targeting Estonian society began, the source of which is attributed to the Russian Federation (Warchol, 2023, p. 312). The initial attacks were chaotic and mainly targeted official government websites, which were disrupted with simple DDoS attacks.

However, by the end of April, the incidents had become more advanced - extensive botnets began to be used (Nowak, 2025, p. 59). In 2015 and 2016, Ukraine fell victim to attacks on electricity systems, resulting in massive power outages (Nowak, 2025, p. 60).

In 2021, a ransomware attack on the Colonial Pipeline company in the United States was highly publicised, temporarily suspending fuel shipments over a large area of the country (Skomra and Wojtasik, 2025, p. 25).

Water pipelines, airports and transportation networks in various European and Asian countries have also become targets of similar actions. The following are the most recent critical infrastructure incidents.

Table 1. *Critical infrastructure cyber incidents in 2024-2025.*

Rok	**Kraj**	**Zdarzenie**
2025	Czech Republic	In May 2025, the Czech Republic accused China of conducting a malicious cyber campaign against the Foreign Ministry. The attacks, attributed to the APT31 group affiliated with China's Ministry of State Security, had been carried out since 2022 and were aimed at espionage and communication disruption (www.reuters.com).
2025	India	Between May 7 and 10, 2025, India experienced over 650 cyber attacks on critical infrastructure, including the energy and transportation sectors. These attacks, attributed to Pakistan-linked entities, were aimed at disrupting essential services at a time of geopolitical tension (ttps://economictimes.indiatimes.com).
2024	USA	Numerous attacks on US water and power systems have been reported in 2024. For example, in January, hackers gained access to control systems at two water utilities in Texas, tampering with pumps and alarms, leading to overflowing reservoirs (www.dni.gov).
2024	USA	In November 2024, American Water, the largest public provider of water and wastewater services in the US, was the victim of a cyber attack. Although water quality was not affected, the company had to disconnect key systems, including its billing platform, highlighting the water sector's vulnerability to cyber threats (www.ibm.com).
2024	Ukraine	In 2024, Russian hacking groups such as KAMACITE and ELECTRUM launched advanced attacks on Ukraine's critical infrastructure, including

		energy, water and heat providers. They used Kapeka malware to access IT networks and took control of OT systems, leading to service disruptions (https://industrialcyber.co).

Source: Own study.

These incidents underscore the growing scale and complexity of cyber threats against critical infrastructure worldwide. In the face of increasingly sophisticated attack techniques and their potential impact on public safety, it is necessary to strengthen protection measures and international cooperation on cybersecurity. These incidents have not only caused direct operational impacts but have also hit public trust and undermined the sense of institutional stability.

Effective management of critical infrastructure security requires implementing a systematic risk analysis. Key elements of this process include identifying essential assets, detecting vulnerabilities, assessing the likelihood and impact of threats, and designing countermeasures and resilience mechanisms. In practice, this means the need for network traffic monitoring tools, security audits, vulnerability scanning, and incident scenario modelling using predictive and AI tools.

Many infrastructure operators still struggle with using outdated industrial control systems, such as SCADA (Control and Data Acquisition Systems), which were not designed with modern cyber threats in mind. Infecting these systems can lead to, for example, shutting down power plants, overloading the grid or halting energy supply. As a result, these attacks can result in serious consequences for critical infrastructure, including the functioning of the state and the economy, as well as the daily lives of individuals (Sadowska, 2023, pp. 12-13).

Lack of updates, difficulties in integrating with modern security, and low levels of network segmentation leave many critical facilities vulnerable to attacks. In addition, the lack of uniform security standards and insufficient incident response procedures increases the risk of threats spreading to other infrastructure segments (Ciekanowski *et al.,* 2024, p. 463)

Cyber threats against critical infrastructure are growing, multidimensional and dynamic. Their effective neutralisation requires not only investment in modern security technologies, but, above all, implementing a security culture based on continuous improvement of procedures, information sharing and knowledge management on a local, national and international scale.

4. A Systems Approach to Critical Infrastructure Security Management

Effective protection of critical infrastructure in the face of growing cyber threats requires an integrated systems approach that combines organisational and technical aspects. CI security and resilience are quite challenging from the point of view of adverse events such as targeted attacks, accidents, and natural disasters (Fujita, Gaeta, Loia, and Orciuoli, 2019).

Key to this context are three concepts related to security management: resilience (resilience), redundancy (redundancy), and business continuity (business continuity). Resilience implies the ability of a system to survive an incident, recover quickly, and adapt to changing threat conditions (Malik *et al.,* 2023).

Redundancy refers to designing systems with backup resources and operation paths that can take over critical functions in a failure (Lezoche, Panetto, 2019). On the other hand, business continuity planning (BCP) is the development of scenarios and procedures to ensure the continuation of critical processes even under conditions of severe disruption.

In the regulatory sphere, European and national legislative initiatives are assuming ever-greater importance. The NIS2 Directive (Network and Information Systems Directive) is of particular significance, as it introduces enhanced obligations concerning risk management and incident response for operators of essential services, technology providers, and public institutions.

Among other requirements, the new provisions mandate the implementation of preventive measures, the conduct of security audits, and the notification of serious breaches to national CSIRTs (Computer Security Incident Response Teams). In Poland, the execution of these tasks is supported, inter alia, by the Governmental CSIRT (CSIRT GOV), the Internal Security Agency, and the national critical infrastructure protection programme coordinated by the Government Centre for Security.

A systemic approach necessitates close collaboration between public and private actors. Because the private sector owns a substantial portion of critical infrastructure, adequate protection requires standardised channels for information exchange, shared response procedures, and interoperable threat-analysis tools.

In this regard, public–private partnerships (PPPs), sector-specific cooperation fora, and international initiatives—within NATO, the European Union, and the European Union Agency for Cybersecurity (ENISA)—play a pivotal role by facilitating the transfer of knowledge, technology, and best practices.

The protection of critical infrastructure also demands the integration of physical and cybersecurity policies. Addressing these domains in isolation can create security gaps that may be exploited through sophisticated hybrid attacks.

Consequently, a robust protection strategy must safeguard physical assets and their ICT components while ensuring organisational preparedness to counter interdisciplinary threats.

Therefore, systemic management of critical infrastructure security in the twenty-first century is not merely a matter of technology; it is a question of the state's and its market partners' organisational capacity to respond jointly to dynamic and increasingly complex threats.

5. Conclusions

Contemporary critical infrastructure constitutes the bedrock of national, societal and economic security. Its operation relies increasingly on digital systems, which, while enabling more efficient delivery of public services, render the infrastructure especially vulnerable to cyber threats.

Advancing digitalisation, integrating ICT systems and deploying cutting-edge technologies—such as the Internet of Things and smart grids—create an environment of vast potential yet heightened risk.

Threat assessments indicate that critical infrastructure is becoming a more frequent target of sophisticated cyberattacks whose scale and complexity are continuously escalating. Ransomware, distributed-denial-of-service (DDoS) campaigns and advanced persistent threats (APTs) can cripple facilities responsible for energy supply, drinking-water provision, healthcare, public transport and financial security.

Particularly alarming is that most incidents stem from security gaps, obsolete technologies and insufficient organisational preparedness for infrastructure operators.

The analysis leads to an unequivocal conclusion: effective management of critical-infrastructure security requires a systemic, strategic approach. The concepts of resilience, redundancy and business continuity are pivotal, jointly enabling the mitigation of attack impacts and restoring normal operations.

Equally critical are implementing new regulations, such as the NIS2 Directive, and expanding institutional (CSIRT, national protection programmes) and competency frameworks within state oversight mechanisms.

It is likewise essential to devise a coherent protection policy that merges the perspectives of physical and cyber security, rather than treating them in isolation. This necessitates integrating security services, operators of essential services, incident-response teams and the private sector, which in many jurisdictions manages a substantial share of critical assets.

Public–private partnerships, information-sharing on threats and vulnerabilities, and international coordination within the EU and NATO should therefore become priorities of state security policy.

Amid intensifying geopolitical pressures, rapid technological change, and a growing incidence of cyber events, states must consistently invest in the resilience of their critical systems. Safeguarding essential infrastructure is not merely a technical challenge; it also reflects institutional maturity and the state's strategic responsibility towards its citizens.

References:

Ciekanowski, Z., Żurawski, S., Wyrębek, H. 2022. Zagrożenia infrastruktury krytycznej. Studia Administracji i Bezpieczeństwa, 13(13), 263-272.

Ciekanowski, Z., Gruchelski, M., Nowicka, J., Żurawski, S., Pauliuchuk, Y. 2023. Cyberspace as a Source of New Threats to the Security of the European Union. European Research Studies Journal, Volume XXVI, Issue 3, pp. 782-797.

Ciekanowski, Z., Nowicka, J., Czternastek, M., Żurawski, S., Mikosik, P. 2024. How Cybersecurity Shapes Effective Organisational Management. European Research Studies Journal, Volume XXVII, Issue 2, pp. 454-464.

Dynes, S., Goetz, E., Freeman, E. 2010. Cyber Security: Are Economic Incentives Adequate? In: Critical Infrastructure Protection, Goetz, E., Shenoi, S., IFIP Advances in Information and Communication Technology. Springer.

Fujita, H., Gaeta, A., Loia, V., Orciuoli, F. 2019. Resilience analysis of critical infrastructures: A cognitive approach based on granular computing. IEEE Trans. Cybern., 49, 1835-1848.

Grima, S., Maditinos, D., Noja, G.G., Stankevičienė, J., Tarczynska-Luniewska, M., Thalassinos, E.I., Nermend, K. (Eds.). 2025. Green Wealth: Navigating towards a Sustainable Future. Emerald Publishing Limited.

Grima, S., Maditinos, D., Noja, G.G., Stankevičienė, J., Tarczynska-Luniewska, M., Thalassinos, E. (Eds.). 2024. Exploring ESG Challenges and Opportunities: Navigating Towards a Better Future. Emerald Publishing Limited.

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.

Lezoche, M., Panetto, H. 2018. Cyber-Physical Systems, a new formal paradigm to model redundancy and resiliency. Enterprise Information Systems, 14(8), 1150-1171.

Malik, M.I., Ibrahim, A., Hannay, P., Sikos, L.F. 2023. Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions. Computers, 12(4), 79.

Milewski, J. 2016. Identyfikacja infrastruktury krytycznej i jej zagrożeń. Zeszyty Naukowe AON, nr 4(105), 99-115.

Narodowym Programie Infrastruktury Krytycznej. 2023.

Nowak, M. 2025. Analiza zagadnień związanych z cyberwojną na podstawie cyberataków na Estonię (2007), ukraińską elektrownię (2015) oraz sieć satelitarną KA-SAT (2022), Tutoring Gedanensis 10(1), 56-64.

Pyznar, M., Abgarowicz, G. 2014. Rola infrastruktury krytycznej w funkcjonowaniu państwa. In: J. Świątkowska, Z. Fałek, (red.), Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny. Instytut Kościuszki, Kraków.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2024 roku.

Raport Roczny z działalności CERT Polska za 2024 rok.

Sadowska, E. 2023. Ewolucja Cyberzagrożeń: Deepfake i Media Syntetyczne w kontekście bezpieczeństwa energetycznego Europy Wschodniej. Studia Wschodnioeuropejskie, t. 2, 8-20.

Skomra, W., Wojtasik, K. 2025. Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK. Terroryzm – studia, analizy, prewencja, wydanie specjalne, 13-34.

Thalassinos, E., Kadłubek, M., Norena-Chavez, D. 2023. Theoretical Essence of Organisational Resilience in Management. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 133-145). 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 (pp. 147-158). Emerald Publishing Limited.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Dz.U. 2007 nr 89 poz. 590.

Warchoł, A. 2023. Od ofiary do światowego lidera. Estonia po cyberatakach z 2007 roku. Politeja, 20(5), 307-327.

Wódkiewicz, R. 2022. Podstawowe zagrożenia funkcjonowania obiektów infrastruktury krytycznej. Zeszyty Naukowe SGSP, Nr 83, 141-161.

X-Force Threat Intelligence Index, Institute for Business Value.