ARCHIVES OF TRANSPORT *ISSN (print):* *0866-9546*
Volume 75, Issue 3, 2025 ***e-ISSN (online):*** *2300-8830*
DOI: *10.61089/aot2025.yfgz9c91*

DIGITAL TECHNOLOGIES AND CYBERSECURITY OF TRANSPORT INFRASTRUCTURE: CHALLENGES FOR RAIL TRANSPORT

Rafał ZGORZELSKI[1], Jakub MURAWSKI[2], Norbert CHAMIER-GLISZCZYŃSKI[3]

[1, 2] Faculty of Transport, Warsaw University of Technology, Warsaw, Poland

[3] Faculty of Economics Sciences, Koszalin University of Technology, Koszalin, Poland

***Abstract**:*

The paper examines the growing importance of cybersecurity in rail transport within the broader framework of critical infrastructure protection. The ongoing digital transformation across all sectors of the economy increasingly affects the functioning of the railway system, which constitutes a strategic component of the national transport network. The adoption of information and communication technologies, as well as industrial automation, has facilitated the deployment of advanced solutions, such as intelligent traffic management systems and predictive maintenance tools, for railway infrastructure. These technologies have significantly enhanced the efficiency, safety, and reliability of transport operations; however, they have also introduced new and complex cybersecurity challenges. The progressive integration of information technology and operational technology systems increases the vulnerability of transport infrastructure to cyber threats that may result in service disruptions, data integrity breaches, or the reduced availability of critical functions. The article underscores the necessity of developing and maintaining an effective cybersecurity management framework in the transport sector, incorporating incident response mechanisms, threat intelligence sharing, and the adoption of standardized procedures and best practices aimed at safeguarding digital assets. Particular attention is devoted to the role of AI as a key driver of digital transformation in the transport sector. Although AI-based technologies enhance operational efficiency and enable greater process automation, their deployment simultaneously introduces a new set of challenges. These challenges primarily relate to data quality and security, system interoperability, and ensuring the transparency and reliability of algorithms used within critical transport infrastructure. The authors emphasize that effective cybersecurity management requires a holistic and integrated approach that combines technical, organizational, legal, and human capital dimensions. Equally important is fostering close cooperation among infrastructure managers, transport authorities, and carriers to ensure a coordinated and resilient cybersecurity framework across the entire transport ecosystem.

Keywords: *cybersecurity, cyber threats, critical infrastructure, ICT systems, cybersecurity management*

To cite this article:

Zgorzelski, R., Murawski, J., Chamier-Gliszczyński, N., (2025). Digital technologies and cybersecurity of transport infrastructure: challenges for rail transport. Archives of Transport, 75(3), 141-158. https://doi.org/10.61089/aot2025.yfgz9c91

Contact:
1) rafal.zgorzelski@pw.edu.pl [https://orcid.org/0009-0000-7719-3662] – corresponding author; 2) jakub.murawski@pw.edu.pl [https://orcid.org/0000-0003-2902-3882]; 3) norbert.chamier-gliszczynski@tu.koszalin.pl[https://orcid.org/0000-0001-7919-0158].

1. Introduction

Critical infrastructure comprises a set of facilities, systems, and resources (both physical and digital) that are essential for ensuring the proper functioning of the state. It includes functionally interconnected buildings, installations, equipment, and services that are of strategic importance to national security, as well as to the efficient operation of the economy and society (Directive 2022/2557 of the European Parliament and of the Council, 2022; Polish Act on crisis management, 2007).

The ongoing digital transformation represents one of the defining characteristics of contemporary society, permeating nearly every aspect of social, economic, and administrative life. Digitalization has profoundly reshaped the functioning of public institutions, enterprises, and individual citizens, influencing everyday communication, management, and decision-making processes. This phenomenon increasingly affects the transport sector, particularly rail transport, which constitutes a critical component of national infrastructure indispensable for maintaining the continuity of state operations (Polish Act on crisis management, 2007; Zgorzelski, 2025).

Modern railways, like other transport systems, are undergoing an intensive process of digital transformation. Information and communication technologies (ICT) and data-driven solutions have become integral components of the operation and management of contemporary railway networks (Poliński & Ochociński, 2020). Digitalization extends across multiple domains, including traffic management, infrastructure maintenance, passenger services, logistics, and rolling stock management. Systems such as the European Train Control System (ETCS), rail traffic management platforms, and predictive maintenance tools have substantially enhanced the efficiency, safety, and reliability of rail operations (Toruń et al., 2019).

The positive impacts of digitalization in rail transport are therefore multifaceted. On one hand, they contribute to improved punctuality, safety, and passenger comfort; on the other, they promote resource efficiency and support the realization of sustainable mobility objectives. However, the ongoing digital transformation also introduces new challenges and risks that are particularly relevant to the rail sector.

The growing integration of operational systems with information technology networks increases the susceptibility of railway infrastructure to cyber threats. Modern railways have become highly dependent on ICT-based systems, making cybersecurity a critical concern. Any incident involving unauthorized data access, system disruption, or manipulation may not only compromise network functionality and erode user trust but, in extreme cases, pose a direct threat to human life and safety (Directive 2022/2557 of the European Parliament and of the Council, 2022; Regulation 2019/881 of the European Parliament and of the Council, 2019).

Fig. 1 presents the relationships between elements of railway infrastructure and potential cyber threats. Railway infrastructure includes both linear objects (such as railway tracks and overhead contact lines) and point objects (such as stations, stops, sidings, loading yards, and intermodal terminals). These physical components are increasingly integrated with digital systems, including data processing centers, telecommunications networks, Internet of Things (IoT) devices, and passenger information systems.

The development and integration of these technologies enhances traffic management efficiency, operational safety, and the overall quality of transport services. However, they simultaneously increase the exposure of infrastructure to a wide range of cyber threats, including network intrusions, malware infections, data breaches, and physical attacks on critical technical facilities. Many of these threats are associated with social engineering techniques, which exploit human factors rather than purely technical vulnerabilities. The consequences of such incidents may include disruptions in control and signaling systems, loss of operational data integrity, and, in severe cases, the interruption of operations across entire sections of the railway network (Krześniak et al., 2022).

In light of the above, ensuring ICT security must be regarded as one of the key challenges facing the modern rail transport system. Effective protection can no longer rely solely on physical safeguards, such as the security of facilities, rolling stock, or railway lines; rather, it must be based on comprehensive and integrated cybersecurity measures. The technologies employed should enable not only the prevention of cyber incidents but also the rapid and effective response to potential attacks when they occur.

Given the ongoing digitalization of critical infrastructure, including railway systems, the development of robust cybersecurity policies, procedures, and competencies has become a priority. Data protection, control system integrity, and operational resilience to disruptions now form the cornerstone of both operational and national security (Górka, 2018). In this context, cybersecurity plays an equally vital role as the physical protection of infrastructure, and its effective implementation requires advanced technological solutions supported by a systemic approach grounded in close cooperation among infrastructure managers, transport authorities, and carriers.

Considering these aspects, the purpose of this article is to analyze the role of cybersecurity in ensuring the continuity and reliability of critical rail transport infrastructure and to identify key challenges and risk management strategies in the face of rapidly evolving digital threats. The article is structured as follows: the first section introduces the issue of ICT security in rail transport; the second discusses the integration of digital technologies and systemic challenges for the sector; the third presents good practices in protecting railway systems against cyber threats; while the subsequent sections analyze specific risk factors and explore the competence and institutional dimensions associated with cybersecurity management. The structure of the article is presented in Fig. 2.

2. Analysis of the integration of digital technologies in rail transport

2.1. Challenges for railways in terms of integrating digital technologies

Fig. 3 presents a general overview of the relationships among key stakeholders within the rail transport system in the context of challenges arising from the integration of digital technologies. Modern railway infrastructure, comprising both technical and ICT components, constitutes the foundation for the provision of transport and logistics services, and its operation directly affects a broad range of stakeholders, including passengers, customers, carriers, transport authorities, and participants in the logistics chain (Murawski et al., 2022). The primary responsibility for ensuring the security and continuity of infrastructure operations lies with railway infrastructure managers, who cooperate with specialized entities tasked with cybersecurity management. These interactions are inherently bidirectional: they involve not only continuous information exchange and incident response but also the planning and implementation of preventive strategies aimed at mitigating emerging cyber threats.

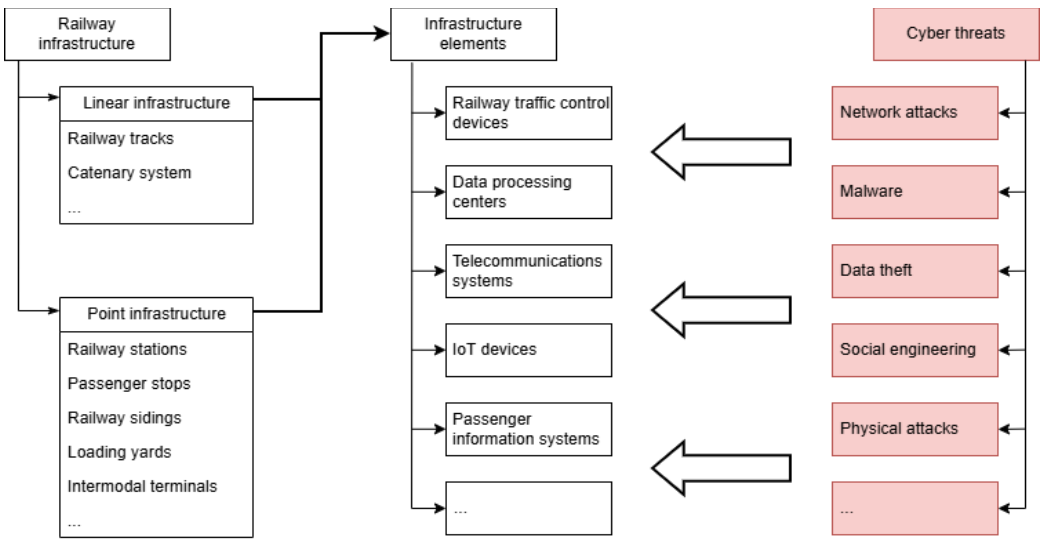

Fig. 1 Potential cyber threats to rail infrastructure (Source: own study)

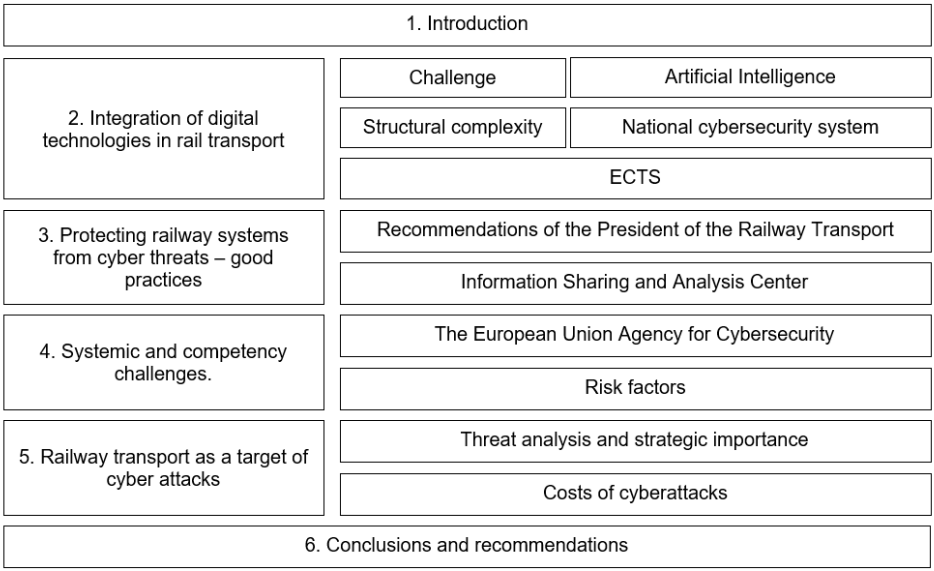

Fig. 2 The article structure (Source: own study)

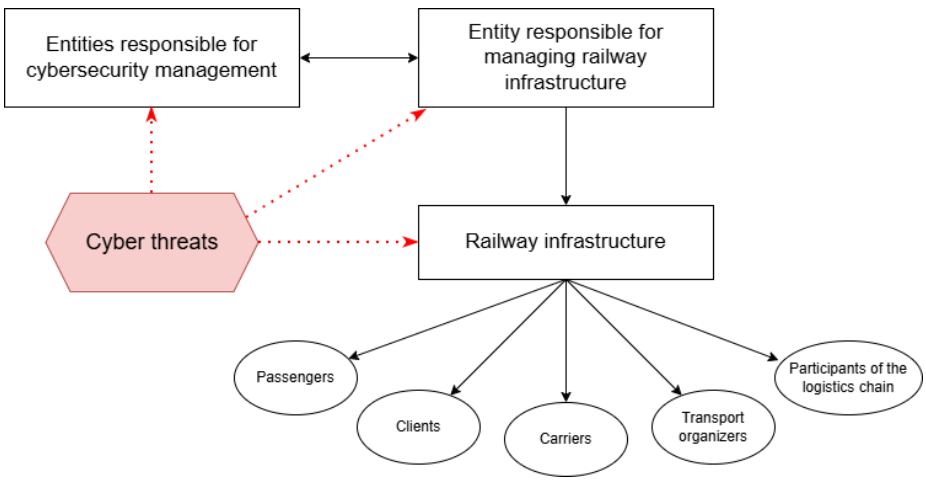

Fig. 3. Relationships between rail transport stakeholders in the context of cyber threats (Source: own study)

Cyber threats can affect railway infrastructure managers by disrupting management and supervision systems, as well as directly compromising elements of the infrastructure itself, including traffic control devices, communication networks, and data processing centers. Regardless of where an incident originates, its consequences tend to propagate throughout the entire railway system, ultimately impacting end users: passengers, carriers, and transport organizers. The framework presented in Fig. 3 underscores the complex nature of the contemporary railway ecosystem, in which the integration of digital technologies necessitates a holistic approach to security management and the establishment of a multi-level cybersecurity protection system (Stypułkowski et al., 2021; Szaciłło et al., 2024).

The ongoing transformation of the railway sector increasingly depends on digitalization, which

underpins the automation of operational processes, enhances system efficiency, and enables the adaptation of services to the growing expectations of end users. Modern railway infrastructure is progressively permeated by ICT and OT systems. These employ advanced, integrated devices capable of real-time communication and include programmable components that directly interact with the physical environment, such as industrial control systems. Consequently, rail transport is becoming part of a broader cyber-physical system, in which the boundaries between the physical and digital domains are gradually disappearing.

While the integration of digital solutions within transport infrastructure brings substantial operational benefits, it simultaneously introduces new cybersecurity risks and challenges related to the protection of IT systems. Modern technologies enable continuous monitoring of railway network status, support traffic management and decision-making processes, and enhance the competitiveness of rail operators. However, their growing complexity also increases exposure to cyber incidents, events that may disrupt or even halt the provision of essential services, including transport operations (Directive 2022/2557 of the European Parliament and of the Council, 2022). Such incidents may involve data theft or loss, interference with control systems, disruptions in service delivery, or acts of sabotage targeting critical infrastructure.

In light of the above considerations, ensuring ICT security must be recognized as one of the key challenges confronting the modern rail transport system. Adequate protection cannot rely solely on physical safeguards, such as the security of facilities, rolling stock, or railway lines, but must instead encompass comprehensive and integrated cybersecurity measures. The technologies employed should support both the prevention of cyber incidents and the capacity for rapid and effective response when such incidents occur.

According to Polish Supreme Audit Office, 2014, cyberspace, understood as a virtual environment formed through the integration of ICT systems that enable the processing, transmission, and storage of information, now represents one of the principal domains of potential offensive activity. As a space where users and systems interact, cyberspace plays a crucial role in the operation of modern transport systems; any breach of its integrity can therefore have a direct impact on operational safety and the continuity of transport services.

Cybersecurity has become one of the fundamental pillars of safe and reliable railway operations, directly influencing the stability of the entire critical infrastructure. It also constitutes an essential component of resilience, understood as the railway system's capacity to prevent, withstand, and respond to incidents, to mitigate their effects, and to efficiently adapt and recover following their occurrence (Ibadah et al., 2024; Maciejewski, 2019).

2.2. Challenges related to artificial intelligence

The development of artificial intelligence (AI) is creating new opportunities for enhancing the safety and reliability management of rail transport infrastructure. Machine learning algorithms can support diagnostic processes, predict failure risks, and strengthen system resilience against both technical and cyber threats. However, the implementation of these technologies in a sector characterized by exceptionally high safety requirements entails numerous technical, organizational, ethical, and legal challenges.

One of the most promising areas of AI application is predictive infrastructure maintenance. Machine learning models, including Long Short-Term Memory recurrent neural networks, enable the analysis of data collected from sensors installed along tracks, bridges, and switches. Such models facilitate the detection of early signs of degradation, the prediction of potential failure times, and the planning of preventive maintenance actions. This predictive approach not only mitigates the risk of accidents but also optimizes maintenance schedules and reduces operational costs (Tang et al., 2022; Xie et al., 2020).

Another important area of AI deployment involves automatic fault detection and track condition monitoring. In this context, advanced deep learning algorithms and Generative Adversarial Networks (GANs) are employed to analyze images obtained from cameras and laser scanners, enabling the identification of cracks, deformations, and misalignments in railway tracks. The high accuracy of image classification models based on GAN techniques significantly reduces the risk of human error in infrastructure inspection processes.

AI is also being increasingly utilized in autonomous traffic control and rolling stock operations. Decision-support systems integrating data from sensors

and cameras allow for the development of autonomous train technologies capable of responding in real time to various events, such as signaling equipment failures, track obstructions, or level crossing malfunctions. AI modules embedded in Automated Driving Systems make it possible to maintain safety levels comparable to those achieved under human supervision (Tang et al., 2022).

Another important area of application involves security monitoring and protection against external threats. AI can analyze data from cameras, environmental sensors, and early warning systems to detect unauthorized access, acts of vandalism, or physical intrusions, as well as to respond to natural hazards such as landslides and floods. The integration of data from multiple sources enhances situational awareness and supports maintenance and security teams in making rapid, data-driven operational decisions.

Despite its considerable advantages, the implementation of AI in the railway sector is accompanied by numerous technological, organizational, and regulatory challenges. A particularly critical issue concerns cybersecurity. The integration of AI systems with IoT infrastructures results in the emergence of so-called AIoT ecosystems, which become potential targets for cyberattacks. Threats may include input data manipulation, system hijacking, or the introduction of malicious learning models. Although AI-based anomaly detection algorithms are increasingly applied, their effectiveness depends heavily on the quality and reliability of training data as well as their robustness to adversarial attacks. Ensuring data integrity and establishing certification mechanisms for AI systems within critical infrastructure currently represent some of the most significant challenges facing rail operators (Qi & Wang, 2025; Semenov et al., 2025).

Another fundamental limitation concerns data quality and security. The performance of machine learning models depends on access to large, diverse, and trustworthy datasets. In practice, sensor data are often incomplete, noisy, or heterogeneous, which hinders their practical use in predictive and diagnostic processes. Moreover, sensitive information related to infrastructure or rail traffic must be protected in compliance with information security and privacy regulations, complicating data processing, sharing, and interoperability among different stakeholders (Davari et al., 2021; Mohammed et al., 2025).

Technical limitations and the absence of interoperability standards also represent critical challenges. Railway systems vary considerably in terms of their architecture, communication protocols, and level of digitalization, which complicates the integration of AI algorithms across heterogeneous operational environments. Moreover, the certification and safety verification of machine learning–based software are significantly more complex than in traditional systems, as the decision-making processes of AI models are often opaque and difficult to interpret.

Equally important are ethical and legal considerations, including accountability for decisions made by autonomous systems, potential biases embedded in training datasets, and the lack of transparency in algorithmic decision-making. Within the context of critical infrastructure, even minor model errors can lead to severe consequences; hence, there is a pressing need to establish a comprehensive regulatory framework that ensures effective oversight and accountability for AI-driven decision processes (Papagiannidis et al., 2025).

AI possesses the potential to substantially enhance the safety, efficiency, and reliability of railway infrastructure through process automation, threat prediction, and decision-support capabilities. However, it simultaneously introduces new categories of risk, particularly in the domains of cybersecurity, data integrity, interoperability, and technological ethics. Therefore, the responsible implementation of AI in the rail sector requires a balanced and systemic approach, encompassing the development of robust certification procedures and the creation of secure, transparent, and explainable algorithms. Only under such conditions can the full potential of AI be realized while maintaining the highest standards of safety and reliability in rail transport infrastructure.

2.3. Structural complexity as a challenge to cybersecurity in the railway sector

In the context of the ongoing digitalization of railway infrastructure and its integration with ICT and OT technologies, a new dimension of systemic complexity is emerging. This complexity arises from the large number of independently operating entities that do not always adhere to uniform standards, procedures, or policies concerning digital security. Such fragmentation significantly hampers the effective management of cybersecurity across the railway

system, increasing the likelihood of protection gaps and inconsistencies.

The liberalization of the railway market in Poland, conducted within the framework of national legislation, reflects broader European trends shaped by the four EU railway packages adopted in 2001, 2004, 2007, and 2016. The first package liberalized the rail freight market and established the principle of separating infrastructure management from the provision of transport services. The second opened the market to international freight transport, the third enabled the liberalization of international passenger transport, and the fourth aims to fully open the domestic passenger market. As a result, the Polish rail market, particularly in the freight transport segment, has become increasingly diverse, encompassing a growing number of operators differing in size, business model, organizational structure, and technological maturity. Similar tendencies are observed across the European Union, although variations in the pace of implementing market liberalization policies have led to differences in the scale and nature of these processes among Member States.

In this environment, it is essential to emphasize that the railway sector, constituting a critical infrastructure of strategic importance to the state, now operates under conditions where escalating cyber threats are compounded by high structural and organizational complexity. The multiplicity of market participants, while beneficial from the perspective of competitiveness and service accessibility, results in the coexistence of numerous, independently managed IT and OT systems. This fragmentation of technological solutions and the absence of uniform standards create substantial challenges for ensuring a coherent and coordinated approach to cybersecurity. The ability to implement adequate preventive measures and to coordinate rapid, collective responses to systemic cyber incidents directly affects the operational safety, business continuity, and overall resilience of the railway system.

2.4. The national cybersecurity system and the railway sector

In Poland, the organization of the national cybersecurity system, including the definition of tasks and responsibilities of its constituent entities, is regulated by legal provisions. According to the Polish Act on the national cybersecurity system (2018), the transport sector is subject to specific competences assigned to the minister responsible for transport, the minister responsible for maritime affairs, and the minister responsible for inland navigation. A key strategic document guiding these activities is the current National Cybersecurity Strategy, which outlines the priorities, objectives, and mechanisms for strengthening digital resilience at both the national and sectoral levels. Furthermore, the position of the Government Plenipotentiary for Cybersecurity has been established to coordinate state policy in this domain and ensure the effective implementation of cybersecurity initiatives.

The institutional framework of Poland's national cybersecurity system comprises three Computer Security Incident Response Teams (CSIRTs) operating at the national level: CSIRT GOV, CSIRT MON, and CSIRT NASK (Table 1). Each of these entities performs specialized functions related to the detection, prevention, and response to cybersecurity incidents within its designated area of responsibility.

Table 1. CSIRTs at the national level (Source: own study based on the Transport Cybersecurity Toolkit (2020))

Name of CSIRT	Leading institution	Responsibility
CSIRT GOV	Head of the Internal Security Agency	Incident response in the systems of government institutions and other public entities of strategic importance; International cooperation in the protection of government infrastructure
CSIRT MON	Minister of National Defence	Supervision of the ICT systems of the Polish Armed Forces and other elements of the infrastructure related to national defense; Cooperation with NATO and allied response structures
CSIRT NASK	Scientific and Academic Computer Network – National Research Institute	Serving the civilian sector, including individual users, educational and research institutions, and essential service providers. Implementing educational and preventive activities

An integral component of CSIRT NASK is CERT Polska, which is responsible for the operational response to network and cybersecurity incidents. The key areas of its activity include the analysis and mitigation of threats related to malware, understood as software or firmware designed to perform unauthorized actions on IT systems, leading to breaches of data confidentiality, integrity, or availability. Such actions may involve device hijacking or the theft of data, passwords, and files through the use of malicious programs such as viruses, worms, Trojan horses, or ransomware.

CERT Polska also conducts extensive activities aimed at identifying and counteracting phishing campaigns, which typically involve the creation of fraudulent websites and the use of social engineering techniques to deceive users into engaging with malicious services. Phishing constitutes a method of illicit data acquisition by impersonating trusted entities. Such attacks can result in unauthorized access to social media accounts, online banking systems, or e-commerce platforms. The attack vectors often include clicking on malicious links, opening infected attachments, or entering login credentials on counterfeit websites that mimic legitimate electronic payment gateways. In addition to its core operational responsibilities, CERT Polska develops and provides free tools that support the security of IT systems and conducts extensive educational and promotional activities aimed at raising public awareness of cybersecurity issues.

The Polish Act on the national cybersecurity system (2018) also provides for the establishment of sectoral cybersecurity teams. In view of the growing scale and complexity of cyber threats affecting the transport sector, the creation of a dedicated sectoral team, with particular focus on the railway subsystem, appears both justified and necessary. Such an entity could play a key role in coordinating information exchange, incident response, and the development of sector-specific security standards.

Although both the existing legislation and strategic cybersecurity documents clearly identify the transport system as a component of the nation's critical infrastructure requiring special protection, they do not sufficiently address the specific characteristics of individual transport modes. This gap is particularly evident in the railway sector, where the current legal framework governing market operations is based mainly on regulations adopted in the early 2000s, an era preceding the rise of contemporary digital threats. Furthermore, ongoing efforts to transpose Directive 2022/2555 of the European Parliament and of the Council (2022) and Directive 2022/2557 of the European Parliament and of the Council (2022) into the national legal system, alongside the revision of the national cybersecurity strategy, present an additional challenge that will determine the effectiveness of future protection mechanisms within the railway sector.

2.5. ETCS in the context of railway safety and cyber threats

In the context of the railway sector, the degree of implementation of the ETCS plays a crucial role. ETCS is an integrated rail traffic control and command system developed under the European Union's European Rail Traffic Management System (ERTMS) program. Its primary objective is to ensure the interoperability of rail transport across the EU, enabling the seamless operation of trains from different operators and rolling stock manufacturers between Member States, regardless of the national signaling and control systems currently in use.

ETCS represents a modern, digital solution based on ICT, designed to progressively replace traditional analog signaling and train control systems. Its deployment contributes to a substantial increase in the automation, safety, and interoperability of railway operations throughout Europe. A key component of ETCS functionality is the radio-stop signal, a digitally transmitted emergency command issued via the GSM-R railway communication network, used in situations that threaten traffic safety.

Notably, unauthorized access to this functionality has been the subject of numerous cybersecurity-related incidents in recent years, attracting significant public and media attention. More broadly, rail traffic control and management systems constitute critical elements of safe railway infrastructure operation. However, the progress of ETCS implementation in Poland remains unsatisfactory. According to Railway Transport Office (2024), in 2023 alone, 728 cases of unauthorized transmission of the radio-stop signal were recorded, an increase of 51.04% (246 incidents) compared with the previous year.

3. Good practices for protecting the railway system against cyber threats

The recommendations of the President of the Railway Transport Office (2025) regarding proper software management in the context of cybersecurity in the rail sector deserve special mention. These recommendations were addressed to railway companies, particularly carriers operating vehicles equipped with on-board IT systems (Table 2).

According to these recommendations, the ongoing digitalization of the railway sector contributes significantly to improving transport safety; however, it is simultaneously associated with the emergence of new threats, particularly those concerning IT infrastructure and on-board vehicle systems.

It is noteworthy that the Information Sharing and Analysis Center for the Railway Sector (ISAC–Kolej), established to coordinate the exchange of information on cybersecurity incidents within the railway subsystem, to develop common security standards and procedures, and to facilitate cooperation with national and international CSIRTs, has developed and adopted two key documents addressing cybersecurity in rail transport: Guidelines on Cybersecurity for Railway Employees (2021) and Guidelines on Cybersecurity of Passenger Rolling Stock (2023).

Table 2. Recommendations regarding protecting the railway system against cyber threats (Source: own study based on the recommendations of the Railway Transport Office, 2025)

Action	Recommendation
Inventory of IT assets	Entities operating railway vehicles should carry out a complete inventory of their IT resources and implement adequate mechanisms for managing them.
Access security overview	Verification of the security of both remote and physical communication interfaces of on-board systems, with particular emphasis on cellular modems and remote service access methods
Risk analysis	Based on the inventory and security review, it was recommended to conduct a risk analysis that would take into account cyber threats throughout the entire life cycle of a railway vehicle.
Restricting remote access	Such access should be limited only to identified, properly secured, monitored, and approved cases.
Securing remote connections	Where remote access is necessary, it is essential to implement appropriate security mechanisms. Particular emphasis should be placed on minimizing the use of private APN (Access Point Name) access points and VPN (Virtual Private Network) connections, while simultaneously employing multi-factor authentication (MFA). Additionally, it was recommended to consider implementing UTM (Unified Threat Management) firewalls, which enable centralized management of security policies and the integration of various security measures within a single platform.
VPN connection location control	Whenever possible, VPN access should be limited to known IP addresses and connections from Poland or other acceptable locations.
System segmentation	Segmentation and micro-segmentation of infrastructure, ensuring separation between OT systems and passenger-accessible systems, and controlling data flows between these environments.
Password management	It was recommended to use strong passwords (at least 12 characters) and eliminate default manufacturer passwords in on-board devices.
Physical access management	It is necessary to develop procedures for controlling physical access to on-board system interfaces, verifying service personnel, and securing devices connected to these systems.
Update management	Wherever possible and after carrying out change management procedures, it was recommended to implement on-board software updates.
Vulnerability management	Regular and proper vulnerability management of inventoried IT assets, including monitoring public databases containing information on detected security vulnerabilities
Contact person	Reporting the contact person to the relevant CSIRT team responsible for handling cybersecurity incidents in the railway sector, and involvement in ISAC–Kolej activities

The first of these documents, based on the Transport Cybersecurity Toolkit (2020), identifies several major categories of cyber threats relevant to the railway sector, including:

1. Malware – software designed to perform unauthorized actions on IT systems, compromising data confidentiality, integrity, or availability;
2. Phishing – attempts to obtain sensitive information by impersonating trusted sources;
3. Distributed Denial of Service (DDoS) – attacks that overwhelm system resources, rendering services unavailable;
4. Denial of Service (DoS) – actions aimed at slowing down or blocking access to resources for authorized users;
5. Data theft – activities aimed at obtaining confidential information, such as login credentials to email or banking systems;
6. Software manipulation – any action intended to alter or disrupt the proper functioning of an application.

It is also worth noting that the European Union Agency for Cybersecurity (ENISA) highlights additional threats relevant to the transport sector, including the railway sector:

1. Ransomware – attacks involving the encryption of data and demands for ransom for its decryption,
2. RDoS (DDoS for Ransom) – threats or actual execution of DDoS attacks to extort ransom, which poses a significant risk to the continuity of services and systems,
3. Spear phishing – personalized social engineering attacks targeting specific individuals or organizations, often highly sophisticated and challenging to detect,
4. Supply chain attacks – exploiting trust in suppliers by infecting components or software, which are then deployed in the infrastructure of the target organization.

According to Protecting Critical Supply Chains: A Guide to Securing Your Supply Chain Ecosystem (2024) the railway sector, these threats cover not only IT systems but also passenger services, ticketing systems, and mobile applications. This necessitates a holistic approach to cybersecurity, encompassing both technical components and the operational and management spheres.

The National Counterintelligence and Security Center (NCSC), the US agency responsible for coordinating counterintelligence activities and national security, highlights the crucial role of supply chain security in protecting critical infrastructure. Analyses prepared by the NCSC emphasize that supply chain manipulation is a key threat to the security of transportation systems – both domestically and internationally. NATO shares a similar view, pointing to the strategic importance of protection against cyber threats targeting components supplied by external suppliers (Kono & Colatin, 2023). According to the Transport Cybersecurity Toolkit (2020), the perpetrators of cyberattacks can be classified into several main categories:

1. State-sponsored groups,
2. Organized cybercrime groups,
3. Hacktivists - individuals acting for ideological or ethical reasons who employ advanced IT skills in ways that violate the law.

The same document also provides recommendations outlining good practices for mitigating the risk of cyberattacks and guidelines for effective incident management, emphasizing the importance of proactive prevention, timely detection, and coordinated response measures.

In the context of threat classification, it is also worth referring to the approach proposed by the Supreme Audit Office (NIK), which distinguishes six types of cyber threats based on the motivations of the perpetrators of cyber activities (Table 3).

Table 3. Classification of threats in cyberspace (Source: own study based on Supreme Audit Office (2025))

Type of cyber threat	Motivation
Cyber hooligans	They act out of curiosity, for fun, or revenge.
Cyber activists	They promote ideas by attacking symbolically, without the intention of financial loss.
Cyber criminals	They operate for profit (fraud, extortion)
Cyber terrorists	Political purpose, intimidation, and destabilization
Cyber spies	Obtaining information for business or intelligence purposes
Cyber soldiers	Military units conducting virtual operations as part of an armed conflict

The Guidelines on Cybersecurity of Passenger Rolling Stock (2023) focuses on the digital protection of passenger rail rolling stock, addressing the specific

risks inherent to this domain as well as the relevant legal and regulatory requirements. The Transport Cybersecurity Toolkit, referenced therein, serves as a practical instrument for raising awareness of cyber threats and strengthening digital resilience across the wider transport sector. Its recommendations are directed toward three primary stakeholder groups: transport personnel, management staff, and cybersecurity specialists.

The document identifies four fundamental categories of threats relevant to transport operations:

1. distribution of malicious software (malware),
2. DoS attacks,
3. unauthorized system access,
4. software manipulation.

In addition, it presents a comprehensive set of recommended countermeasures tailored to the characteristics of different transport modes, while accounting for the structural and organizational diversity of entities within the sector, irrespective of their size.

The detailed approach proposed by the ENISA identifies a range of risk factors that are equally relevant to the security of railway systems (Table 5). These factors highlight the interdependencies between technological, organizational, and human elements that shape the overall cybersecurity posture of transport infrastructure.

From the perspective of the average IT system user, whether in a professional or private context, additional vulnerabilities often arise from insufficient cyber hygiene practices. These include behaviors such as the use of weak passwords, failure to update software, or uncritical handling of email attachments and hyperlinks, all of which can contribute to the escalation of cybersecurity risks within the broader rail transport ecosystem.

4. Systemic and competency challenges. Risk analysis and international initiatives

ENISA identifies the most important challenges related to cybersecurity of rail transport, classifying them into several basic categories (Table 4).

An analysis of available reports clearly indicates that one of the key challenges in the field of cybersecurity is the shortage of qualified specialists and the lack of systematic, professional training programs. This issue also affects the railway sector, which has begun implementing a number of initiatives aimed at strengthening cybersecurity competencies.

Among these initiatives are projects carried out under the auspices of the International Union of Railways (UIC). One example is the CYRUS project (Personalized and Needs-Based Workplace Training Programmes Enhancing Cybersecurity Skills Across Industrial Sectors), which seeks to identify existing competency gaps and to develop personalized training programs tailored to the specific needs of the railway industry. Another significant initiative is the CYRAIL project (Cybersecurity in the Railway Sector), which focuses on detecting threats and designing mechanisms to prevent and mitigate cyberattacks on railway systems.

Table 4. Key challenges in rail transport cybersecurity, according to ENISA (Source: own study based on Liveri et al. (2020))

Challenge	ENISA's position
Complexity of legal provisions	Cybersecurity regulations are often complex to interpret and implement, which hinders uniform and effective actions in the railway sector.
Insufficient awareness of the need to strengthen cybersecurity	There is a lack of knowledge about the scale and effects of potential threats among both decision-makers and operational staff.
Technological challenges	New technologies increase efficiency, but at the same time, they bring new threats that require appropriate security mechanisms.
Distributed systems and outdated infrastructure	A large number of systems operating in different locations, often based on outdated solutions, creates security gaps that are difficult to manage.
The need for further digitalization while maintaining a high level of security	Railways must continue their digital transformation to remain competitive, but this cannot come at the expense of cybersecurity.

Table 5. Significant risk factors affecting the safety of railway systems (Source: own study based on European Union Agency for Cybersecurity (2024), Szaciłło et al. (2021) and the authors' own experiences)

Risk factors, according to ENISA, that are significant for the safety of railway systems	Risk factors from the point of view of the user of IT systems
Supply chain integrity breaches, particularly those related to threats from third-party software	Taking risky actions on work and personal devices
Shortage of cybersecurity specialists	Lack of regular safety testing
Susceptibility of systems to human error, especially in the context of using outdated components in complex cyber-physical systems	Not backing up your data regularly.
Using outdated technologies in a complex and overloaded cross-sector environment	Using untrusted Wi-Fi networks
Growing risk of digital surveillance and threats to user privacy	Using mobile devices of unknown origin
Dependence on cross-border ICT service providers who may constitute single points of failure	Using outdated or low-quality antivirus software
Development of advanced disinformation campaigns and influence operations	No software updates
The escalation of hybrid threats, combining physical, digital and psychological elements	Lack of knowledge of the user, who often relies on unreliable sources of information
Potential abuses related to the use of AI	Using the same (or weak) passwords for multiple accounts
Physical effects of environmental disruptions affecting critical infrastructure	No two-factor authentication (2FA)

In addition, the UIC Cybersecurity Solution Platform (CSSP) serves as an interdisciplinary forum that brings together experts from various domains to systematically support the railway sector in identifying, assessing, and implementing modern cybersecurity solutions. It is worth emphasizing that these projects form only part of UIC's broader efforts to strengthen the cybersecurity posture of the global railway community. Within the UIC framework, a dedicated COLPOFER working group operates to enhance cooperation among railway undertakings and infrastructure managers in the field of security, while its WC Cyber Crime subgroup focuses specifically on issues related to information technology and cyber protection in the railway sector.

5. Railway transport as a target of cyber attacks - statistical data

5.1. Threat analysis and strategic importance

According to Lella et al. (2024) the transport sector, including rail, was the second most frequently targeted area for cyberattacks within the European Union, accounting for approximately 11% of all reported cybersecurity incidents. Only the public administration sector, representing 19% of incidents, recorded a higher share, while the transport sector surpassed the financial sector, which accounted for 9% of reported cases. These findings are broadly consistent with analyses conducted by national institutions monitoring cyber threats in Poland, although certain variations can be attributed to specific local conditions. Similar conclusions have also been drawn by international organizations and research institutes, confirming that the transport sector, particularly the railway subsystem, should be considered a strategic priority for cybersecurity policy at both national and EU levels.

In this context, the NIS 2 Directive (Directive 2022/2555 of the European Parliament and of the Council, 2022) underscores the need to strengthen cybersecurity protection across all modes of transport, including aviation, maritime, rail, and road. However, it is not only the number of cyber incidents that determines the sector's vulnerability, but more importantly, the magnitude of their potential impact. As highlighted in the educational materials developed jointly by the NCSC and the Cybersecurity and Infrastructure Security Agency critical infrastructure, including the transport sector, forms the foundation of the national economy. Its protection is therefore essential for maintaining public safety, national security, and overall resilience.

According to the National Counterintelligence and Security Center (2024), sectors such as communications, energy, financial services, transportation, and water management are so deeply interconnected that

disruptions in one can trigger cascading effects across others. Polish researchers also emphasize this interdependence, particularly in the context of hybrid and cyber threats, which amplify the systemic vulnerability of national infrastructure (Kołodziejczyk, 2020; Łukasiewicz & Szlachter, 2025; Milewski, 2016; Smagowicz et al., 2021]. Disruptions in the functioning of automated control systems or ICT networks can have far-reaching consequences for state stability and societal well-being, making cybersecurity an indispensable pillar of infrastructure protection and a fundamental component of national resilience (Molendowska et al., 2021).

5.2. Consequences for transport security and the costs of cyberattacks

The escalating scale of cybersecurity challenges is clearly evidenced by recent statistical data. According to Federal Bureau of Investigation (2025), in the United States, financial losses resulting from cyberattacks reached a record USD 16.6 billion in 2024, with ransomware incidents accounting for the largest share of these losses. Both the frequency and sophistication of such attacks continue to grow worldwide, including in Poland. Although comprehensive data on the total financial impact of cyberattacks, particularly within the railway sector, are not yet available, valuable insights into the scale and dynamics of cybercrime can be drawn from the operational statistics of the Central Bureau for Combating Cybercrime (CBZC).

CBZC data provide a partial yet revealing picture of cybercrime activity in Poland. In 2023, the Bureau conducted 619 preparatory proceedings, detaining 501 individuals, of whom 231 were remanded in custody. During these operations, assets worth PLN 441.3 million were seized, and property valued at PLN 14.3 million was recovered. In 2024, the number of recorded cases almost doubled to 1,253, leading to the detention of 848 individuals, including 312 placed under temporary arrest. Assets worth an estimated PLN 72.7 million were secured, while PLN 49.7 million was successfully recovered. The above data are presented in Fig. 4 and 5.

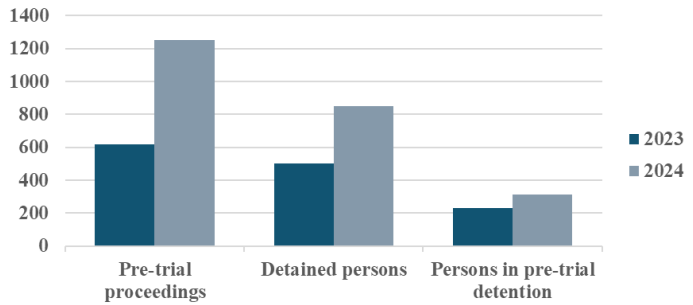

Fig. 4. Operational statistics of the Central Bureau for Combating Cybercrime in 2023-2024 (Source: own study based on Central Bureau for Combating Cybercrime)

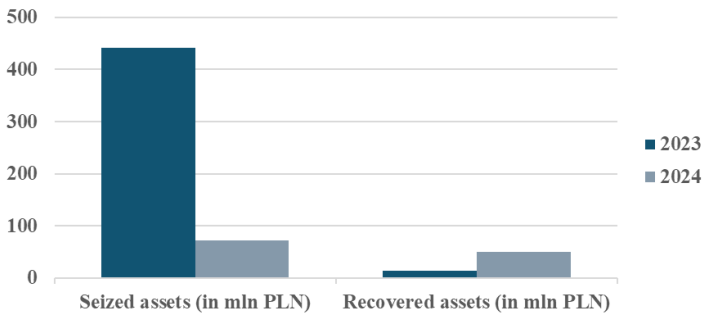

Fig. 5. Financial statistics of the Central Bureau for Combating Cybercrime in 2023-2024. (Source: own study based on Central Bureau for Combating Cybercrime)

According to the Microsoft Digital Defense Report 2024: The Foundations and New Frontiers of Cybersecurity, Poland ranks third in Europe, after Ukraine and the United Kingdom, in terms of exposure to cybersecurity threats. On the global scale, Poland occupies ninth place, alongside India, following the United States, Israel, the United Arab Emirates, Ukraine, the United Kingdom, Taiwan, and South Korea. Forecasts concerning the global cost of cybercrime are alarming: total losses are expected to reach USD 10.5 trillion by 2025.

In the second quarter of 2025, Poland was identified as the most frequently targeted European country for hacktivist attacks, according to a report published by the Spanish Industrial Cybersecurity Center (ZIUR – Gipuzkoa Industrial Cybersecurity Center). This institution, established by the Gipuzkoa Provincial Council, supports industrial enterprises in developing digital security capabilities. In the analyzed ranking, Poland surpassed countries such as Ukraine, the United Kingdom, France, Germany, the Netherlands, Finland, Lithuania, Romania, and Israel.

Further evidence of the growing scale of digital threats is provided by operational data from national cybersecurity institutions. According to Internal Security Agency (2024), in 2024, CSIRT GOV registered 17,439 reports of potential incidents, of which 3,991 were classified as actual cybersecurity threats. During the same period, CERT Polska handled 103,449 incidents, including 565 related to the transport sector. Among these, 57 incidents (two of which were associated with transport) were assessed as potentially capable of causing serious service degradation or complete disruption of essential operations (NASK - National Research Institute, 2025).

It is also worth emphasizing that the digital market within the European Union is estimated at approximately EUR 3 trillion, representing about 20% of the EU's GDP. This scale underscores the need for a systemic approach to digital security at the EU level. One of the principal regulatory instruments in this domain is the NIS 2 Directive, which encompasses around 350,000 enterprises and organizations classified as essential or important to the functioning of the Union's economy and society (CISCO, 2023).

According to Allied Market Research (2021), in the context of the railway sector, the global cybersecurity market was valued at USD 7.73 billion in 2020, with forecasts projecting growth to approximately USD 14.69 billion by 2030, reflecting the increasing recognition of cybersecurity as a strategic investment area within the digital transformation of transport systems.

6. Conclusions

Based on the analyses and considerations presented in this article, a set of conclusions and strategic recommendations has been formulated concerning the security of rail transport in the context of ongoing digitalization and the growing spectrum of cyber threats.

Rail transport is a fundamental component of critical infrastructure, performing essential functions in both civilian and military contexts. Its significance extends beyond the mere transport of passengers and goods: the railway system underpins the continuity of state operations, supports economic stability, and plays a vital role in crisis management and defense activities. As a complex socio-technical system, the modern railway network is increasingly interlinked with ICT infrastructure and digital management platforms, whose reliability and resilience directly determine the overall safety and operational stability of the sector.

The integration of advanced digital technologies into railway infrastructure brings substantial benefits, including enhanced operational efficiency, system reliability, and improvements in maintenance and traffic management processes. Solutions based on data analytics, automation, and real-time communication enable more precise planning, early detection of irregularities, and rapid responses to emerging threats. However, increasing digitalization simultaneously introduces new and complex cybersecurity challenges. The scale, sophistication, and interdependence of these threats make the protection of IT and telecommunications systems a strategic priority and a key determinant of the resilience of the rail sector. AI is gaining particular importance in this context, offering the potential to significantly enhance the safety, efficiency, and reliability of rail operations. Machine learning algorithms can be applied to predictive infrastructure maintenance, data analysis from sensors and cameras, track fault detection, and train traffic control. These technologies enable the early identification of anomalies and the mitigation of risks, contributing to greater reliability and preventive maintenance efficiency. Nevertheless, the

implementation of AI also introduces new risks, especially in relation to cybersecurity, data quality and integrity, interoperability, and accountability for decisions made by autonomous systems.

The responsible deployment of AI requires a balanced and transparent approach, encompassing the development of certification and validation methods, the creation of secure and explainable algorithms, and close cooperation between infrastructure managers, transport authorities, and railway undertakings. Only such an integrated approach will allow full realization of AI's potential while maintaining the highest safety and reliability standards in railway operations.

The development of next-generation railways will increasingly depend on advanced IT technologies and robust cybersecurity frameworks. The quality and resilience of these systems will determine both the security and operational continuity of the transport network. Therefore, modern and future railways must rely on well-designed digital defense architectures, supported by AI-driven systems for monitoring, communication, and infrastructure management.

A comprehensive approach to security is essential, one that extends beyond the physical protection of facilities, rolling stock, and railway lines, and incorporates integrated ICT security management. Infrastructure protection should be based on a coherent model combining incident prevention, threat detection, rapid response, and efficient restoration of business continuity after disruptions.

A major challenge in Poland remains the fragmented structure of the railway sector, characterized by numerous independent entities operating under different standards and procedures. The absence of a coordinated cybersecurity framework hinders effective incident management, limits information exchange, and constrains the capacity for a unified response to cyber threats. Addressing this fragmentation is crucial to building a resilient, interoperable, and secure digital railway ecosystem.

To counter the growing scale of cyber threats, it is advisable to establish a specialized CSIRT dedicated to the transport sector, with particular focus on rail transport. Such a body could coordinate preventive actions, conduct risk assessments, and support operators in incident response, information sharing, and capacity building for sector-wide resilience.

Simultaneously, it is necessary to adapt legal frameworks and strategic documents to the specific conditions of the railway sector, its organizational, technical, and operational characteristics. Regulations on cybersecurity and interoperability should reflect the expanding role of digitalization and emerging technologies, including AI. This requires a systematic update of both national and EU strategic documents to align them with current technological and operational realities.

An equally important component of resilience building is the development of competencies and cybersecurity awareness. Enhancing safety requires sustained efforts to raise threat awareness among both management and operational staff, accompanied by methodically planned training and educational programs.

The railway sector also faces major technological and infrastructural challenges, including the modernization of outdated systems, the integration of dispersed digital solutions, and investment in advanced technologies. The deployment of the ETCS represents an important step toward achieving greater interoperability, automation, and safety within the European rail transport network.

In conclusion, the future of a modern and secure railway system depends on the effective integration of digitalization, AI-based innovation, robust cybersecurity mechanisms, and highly skilled personnel. Only a comprehensive and responsible strategy, combining technology, regulation, and education, will enable the railway sector to fully leverage the opportunities of digital transformation while ensuring the resilience and security of critical transport infrastructure.

References

1. Bańka, M., Daniłowski, J., Czerliński, M., Murawski, J., Żochowska, R., & Sobota, A. (2022). A Feedback Analysis Automation Using Business Intelligence Technology in Companies Organizing Urban Public Transport. *Sustainability*, 14(18), 11740. https://doi.org/10.3390/su141811740
2. Cyberbezpieczeństwo na kolei - Rekomendacje Prezesa UTK. Urząd Transportu Kolejowego. Retrieved August 17, 2025, from https://utk.gov.pl/pl/aktualnosci/19920,Cyberbezpieczenstwo-na-kolei-rekomendacje-Prezesa-UTK.html

3. Davari, N., Veloso, B., Costa, G. D. A., Pereira, P. M., Ribeiro, R. P., & Gama, J. (2021). A Survey on Data-Driven Predictive Maintenance for the Railway Industry. *Sensors*, 21(17), 5739. https://doi.org/10.3390/s21175739
4. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA Relevance), EP, CONSIL, 333 OJ L (2022). http://data.europa.eu/eli/dir/2022/2555/oj
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 (Text with EEA Relevance), EP, CONSIL, 333 OJ L (2022). http://data.europa.eu/eli/dir/2022/2557/oj
6. FBI Releases Annual Internet Crime Report. Federal Bureau of Investigation. Retrieved August 18, 2025, from https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report
7. Foresight Cybersecurity Threats For 2030 – Upadate. Executive Summary. (2024). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024
8. Górka, M. (2018). Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa. In T. Dębowski (Ed.), *Cyberbezpieczeństwo wyzwaniem XXI wieku*. Wydawnictwo Naukowe Archae-Graph.
9. Ibadah, N., Benavente-Peces, C., & Pahl, M.-O. (2024). Securing the Future of Railway Systems: A Comprehensive Cybersecurity Strategy for Critical On-Board and Track-Side Infrastructure. *Sensors*, 24(24), 8218. https://doi.org/10.3390/s24248218
10. Informe de ciberinteligencia industrial del tercer trimestre. ZIUR. Retrieved August 8, 2025, from https://www.ziur.eus/eu/-/informe-trimestral-de-tendencias-sobre-ciberinteligencia-industrial
11. Kołodziejczyk, R. (2020). Bezpieczeństwo Rzeczypospolitej Polskiej w cyberprzestrzeni, w: Bezpieczeństwo w cyberprzestrzeni. In M. Molendowska & R. Miernik (Eds.), *Bezpieczeństwo w cyberprzestrzeni: Wybrane zagadnienia* (pp. 188–201). Wydawnictwo Adam Marszałek.
12. Kono, K., & Colatin, S. de T. (2023). National Approaches to the Supply Chain Cybersecurity: Taking a More Restrictive Stance Against High-Risk Vendors. https://ccdcoe.org/library/publications/national-approaches-to-the-supply-chain-cybersecurity-taking-a-more-restrictive-stance-against-high-risk-vendors/
13. Krześniak, M., Jacyna, M., Pryciński, P., Murawski, J., & Bańka, M. (2022). Business Environment Of Rail Transport In The Context Of The Value Chain. *Scientific Journal of Silesian University of Technology. Series Transport*, 116, 179–195. https://doi.org/10.20858/sjsutst.2022.116.11
14. Lella, I., Theocharidou, M., Magonara, E., Malatras, A., Svetozarov Naydenov, R., Ciobanu, C., & Chatzichristos, G. (Eds.). (2024). ENISA Threat Landscape 2024 July 2023 to June 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
15. Liveri, D., Theocharidou, M., & Naydenov, R. (2020). Railway cybersecurity. Security measures in the Railway Transport Sector. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/railway-cybersecurity
16. Łukasiewicz, J., & Szlachter, D. (2025). Prawne i techniczne metody ochrony obiektów infrastruktury krytycznej przed zagrożeniami ze strony bezzałogowych statków powietrznych – przykład Polski. *Terroryzm*, 167. https://doi.org/10.4467/27204383TER.25.006.21509
17. Maciejewski, R. (2019). Ochrona infrastruktury krytycznej – narracje prawne i politologiczne. Fnce sp. z o.o.
18. Microsoft Digital Defense Report 2024. (2024). Microsoft. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024
19. Milewski, J. (2016). Identyfikacja infrastruktury krytycznej i jej zagrożeń. *Zeszyty Naukowe AON*, 4(105), 99–115.

20. Mohammed, S., Budach, L., Feuerpfeil, M., Ihde, N., Nathansen, A., Noack, N., Patzlaff, H., Naumann, F., & Harmouch, H. (2025). The effects of data quality on machine learning performance on tabular data. *Information Systems*, 132, 102549. https://doi.org/10.1016/j.is.2025.102549
21. Molendowska, M., Górski, P., & Zal, P. (2021). Logistyka bezpieczeństwa. Wybrane zagadnienia. Wydawnictwo Adam Marszałek.
22. Murawski, J., Szczepański, E., Jacyna-Gołda, I., Izdebski, M., & Jankowska-Karpa, D. (2022). Intelligent mobility: A model for assessing the safety of childrentraveling to school on a school bus with the use of intelligent bus stops. *Eksploatacja i Niezawodność – Maintenance and Reliability*, 24(4), 695–706. https://doi.org/10.17531/ein.2022.4.10
23. Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems*, 34(2), 101885. https://doi.org/10.1016/j.jsis.2024.101885
24. Poliński, J., & Ochociński, K. (2020). Cyfryzacja w transporcie kolejowym. *Problemy Kolejnictwa*, z. 188. https://doi.org/10.36137/1885P
25. Protecting Critical Supply Chains: A Guide to Securing Your Supply Chain Ecosystem. (2024). The National Counterintelligence and Security Center. https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats
26. Qi, J., & Wang, J. (2025). Bridging Artificial Intelligence and Railway Cybersecurity: A Comprehensive Anomaly Detection Review. *Transportation Research Record: Journal of the Transportation Research Board*, 2679(5), 232–255. https://doi.org/10.1177/03611981241302335
27. Railway Cybersecurity Market Expected to Reach $14.69 Billion by 2030. (2021). Allied Market Research. https://www.alliedmarketresearch.com/press-release/railway-cybersecurity-market.html?utm
28. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 r. (2025). Agencja Bezpieczeństwa Wewnętrznego. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/983,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2024-roku.html
29. Raport roczny z działalności CERT Polska w 2024 roku. (2025). NASK - Państwowy Instytut Badawczy. https://cert.pl/posts/2025/04/raport-roczny-2024/
30. Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej. (2025). Najwyższa Izba Kontroli. https://www.nik.gov.pl/kontrole/P/14/043
31. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA Relevance), 151 OJ L (2019). http://data.europa.eu/eli/reg/2019/881/oj
32. Safeguarding Our Critical Infrastructure. (2024). National Counterintelligence and Security Center. https://www.dni.gov/index.php/ncsc-how-we-work/203-about/organization/national-counterintelligence-and-security-center/2762-safeguarding-our-future?utm
33. Semenov, I., Jacyna, M., Auguściak, I., & Wasiak, M. (2025). Hybrid Human–AI Collaboration for Optimized Fuel Delivery Management. *Energies*, 18(19), 5203. https://doi.org/10.3390/en18195203
34. Smagowicz, J., Szwarc, K., Kisilowski, M., Wiśniewski, M., & Skomra, W. (2021). Zarządzanie bezpieczeństwem infrastruktury krytycznej i ciągłością usług kluczowych państwa. Oficyna Wydawnicza Politechniki Warszawskiej.
35. Sprawozdanie ze stanu bezpieczeństwa ruchu kolejowego 2023 r. (2024). Urząd Transportu Kolejowego https://utk.gov.pl/pl/dokumenty-i-formularze/opracowania-urzedu-tran/21639,Sprawozdanie-ze-stanu-bezpieczenstwa-ruchu-kolejowego-2023-r.html
36. Stypułkowski, K., Gołda, P., Lewczuk, K., & Tomaszewska, J. (2021). Monitoring System for Railway Infrastructure Elements Based on Thermal Imaging Analysis. *Sensors*, 21(11), 3819. https://doi.org/10.3390/s21113819
37. Szaciłło, L., Jacyna, M., Szczepański, E., & Izdebski, M. (2021). Risk assessment for rail freight transport operations. *Eksploatacja i Niezawodność – Maintenance and Reliability*, 23(3), 476–488. https://doi.org/10.17531/ein.2021.3.8

38. Szaciłło, L., Krześniak, M., Zgorzelski, R., Lasota, M., & Franke, P. (2024). Resistance And Safety Of The Railway Transport System In The Context Of Disruptions Occurring During Rail Freight Transportation. *Transport Problems*, 19(2), 191–204. https://doi.org/10.20858/tp.2023.19.2.15
39. Tang, R., De Donato, L., Bešinović, N., Flammini, F., Goverde, R. M. P., Lin, Z., Liu, R., Tang, T., Vittorini, V., & Wang, Z. (2022). A literature review of Artificial Intelligence applications in railway systems. *Transportation Research Part C: Emerging Technologies*, 140, 103679. https://doi.org/10.1016/j.trc.2022.103679
40. Toruń, A., Sokołowska, L., & Jacyna, M. (2019). Communications-based train control system—Concept based on WiFi LAN network. *Proceedings of the International Conference Transport Means 2019*, 911–915.
41. Transforming NIS2. Challenge sito Strategic Opportunities. A Cisco Perspective. (2023). CISCO. https://www.cisco.com/c/m/en_emea/products/security/nis2-directive.html#~guide-to-nis2
42. Transport Cybersecurity Toolkit (2020). European Commission. Mobility and Transport. https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en
43. Ustawa z Dnia 5 Lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (2018). https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560
44. Ustawa z Dnia 26 Kwietnia 2007 r. o zarządzaniu kryzysowym (2007). https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20070890590
45. Wyniki statystyczne Centralnego Biura Zwalczania Cyberprzestępczości za 2023 rok. (2024). Centralne Biuro Zwalczania Cyberprzestępczości. https://cbzc.policja.gov.pl/bzc/statystyka/raporty-z-dzialalnosci/262,Raporty-z-dzialalnosci.html
46. Wyniki statystyczne Centralnego Biura Zwalczania Cyberprzestępczości za 2024 rok. (2025). Centralne Biuro Zwalczania Cyberprzestępczości. https://cbzc.policja.gov.pl/bzc/statystyka/raporty-z-dzialalnosci/262,Raporty-z-dzialalnosci.html
47. Wytyczne dot. Cyberbezpieczeństwa dla pracowników podmiotów kolejowych. (2021). https://isac-kolej.pl/publikacje.html
48. Wytyczne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego, wersja 1.0. (2023). https://isac-kolej.pl/publikacje.html
49. Xie, J., Huang, J., Zeng, C., Jiang, S.-H., & Podlich, N. (2020). Systematic Literature Review on Data-Driven Models for Predictive Maintenance of Railway Track: Implications in Geotechnical Engineering. *Geosciences*, 10(11), 425. https://doi.org/10.3390/geosciences10110425
50. Zgorzelski, R. (2025). Zarządzanie procesowe w sytuacjach kryzysowych. In A. Bitkowska, M. Kruk, & J. Smagowicz (Eds.), Potencjał Zarządzania Procesowego Strategie-Ludzie-Technologie. TNOiK „Dom Organizatora”.