Riding the digital rails: safeguarding

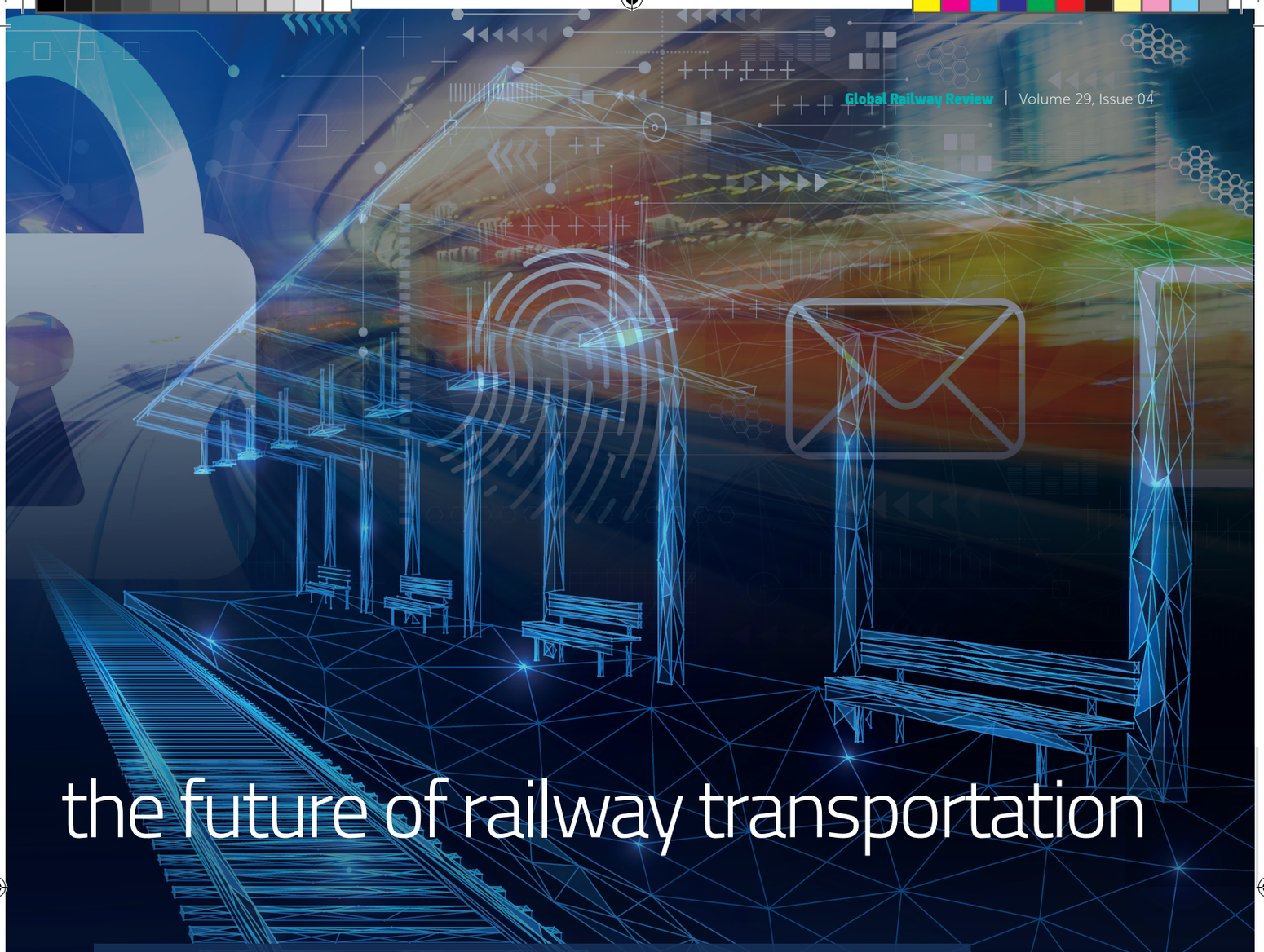
For the majority of its history, the railway sector was a closed industry that slowly embraced new technologies. In terms of its previous operation, a key focus in both legislative and executive levels was on safety requirements, defined by EU regulations as the freedom from unacceptable risk of harm. Safe railways have been a domain of the EU for many years, as evident in various legal acts such as safety directives, interoperability directives, and the regulation regarding CSM RA.

MODERN RAILWAYS are becoming open and interoperable systems. Within the EU, a series of legislative initiatives have been taken to create a Single European Railway Area, where rail transport can operate seamlessly, with hurdles removed through railway digitisation. This process aims to facilitate operations for various entities, particularly infrastructure managers, carriers and railway equipment manufacturers.

Railway infrastructure primarily relies on computer networks, both wired and wireless. This means it may be vulnerable to cyber-attacks, and a wide range of entities are susceptible to such attacks. Each entity operating in the railway market possesses certain data, which can be classified as sensitive information. For instance, freight carriers may transport dangerous goods. All information, such as the train schedule for such cargo, is a potential target for an attack.

This article serves as a starting point for further considerations on cyber-security in railway transportation. It is crucial to note that this is an issue that already holds significant importance in the entire transport sector. Recent events in Poland involving an unauthorised activation of the 'Radio-STOP' signal, which immobilises all railway vehicles in a specific area, demonstrate the critical importance of securing the railway system. Of course, it is challenging to label this as a cyber-attack, especially since 'Radio-STOP' is not a digital but an analog system. However, when considering the potential negative consequences, such as a tragic railway accident, the conclusions are clear. Railway

> *"It is crucial to note that this is an issue that already holds significant importance in the entire transport sector."*



the future of railway transportation

infrastructure, especially railway traffic control devices, should be adequately secured.

In the European Union, emphasis has been placed on the installation of digital railway traffic control devices, which are part of the ERTMS system. It is worth mentioning that a new Commission Implementing Regulation (EU) 2023/1695 of 10 August 2023 on the technical specification for interoperability relating to the control-command and signalling subsystems of the rail system in the European Union and repealing Regulation (EU) 2016/919.

Cyber-security is a relatively new issue in the railway sector, yet we are already able to identify many cyber-attacks on railway infrastructure. In its November 2021 report on Railway Cybersecurity Good Practices in Cyber Risk Management, ENISA (European Union Agency for Cybersecurity) presented several possible attack scenarios on railway infrastructure. One of them pertains to an attack on traffic control systems.

In contrast, in the report 'Railway Cybersecurity: Security Measures in the Railway Transport Sector', the ENISA notes that until 2020, the subsector of railway transport was not a direct target of cyber-criminal attacks. Nevertheless, between 2015 and 2020, various incidents occurred in different European countries, drawing attention to the sector's vulnerability. Some of these incidents included:

1. Data leak from passenger Wi-Fi networks on British trains – the leak involved email addresses and travel information of about 10,000 passengers who used the open Wi-Fi network
2. Malware attack on the Swiss railway company Stadler – the company's systems were infected with malware that enabled the theft of sensitive data. After the company refused to pay a ransom, the criminals published the stolen data and internal documents online
3. Ransomware attack on the Spanish high speed infrastructure manager – ADIF was targeted by ransomware, allowing for the theft of gigabytes of personal and business data.

ENISA's report also refers to the NIS1 directive, which has now been replaced by the NIS2 directive, imposing specific obligations that both EU member states and entities in the sector must adhere to.

Above all, the entire transport sector has been defined in the directive as a critical sector, meaning its operation is essential from the EU's perspective. The provisions of the directive will apply to all railway infrastructure managers. As for railway carriers and operators of service facilities, their size must be taken into account. If a given company exceeds the thresholds set for medium-sized enterprises, it

> *In the report 'Railway Cybersecurity: Security Measures in the Railway Transport Sector', the ENISA notes that until 2020, the subsector of railway transport was not a direct target of cyber-criminal attacks.*

will be bound by the directive's provisions and the corresponding national regulations issued on its basis.

In addition to regulatory changes, other actions have also been taken. In particular, the European Railway-ISAC has been established as a platform for exchanging analyses and information for the railway sector. This initiative brings together experts in information and cyber-security, focusing on the security of industrial control systems and IT infrastructure in railways. ISAC operates as a public-private partnership, uniting entities interested in sharing knowledge about threats in the railway transport sector.

Furthermore, within CENELEC, the standard CLC/TS 50701, the first international standard providing cyber-security guidance for rail applications, has been developed. This standard addresses how cyber-security should be managed for operators and product providers in the railway subsector. Based on this specification, ENISA released publicly available guidelines on 'Zoning and Conduits for Railways' in February 2022.

It is important to note that the NIS2 directive should be read in conjunction with TS50701, as these documents are, to some extent, interconnected. TS50701 complements the requirements of the directive and provides valuable guidance for meeting NIS2 requirements. Additionally, TS50701 also refers to the EN50126 RAMS standard.

For instance, one of the basic obligations for entities covered by NIS2 will be to implement a risk management policy in cyber-security. National regulations should specify which technical, operational, and organisational measures should be taken. The directive only outlines their framework. Risk management measures should be proportional to the identified cyber threat. At the same time, these measures should consider current knowledge, as well as applicable standards and implementation costs.

The new regulation on the TEN-T network also holds significant importance. It imposes specific obligations on infrastructure managers, carriers and intermodal transport operators. The regulation sets ambitious deadlines for the installation of the radio-based ERTMS system and the development of ICT applications for the exchange of information necessary for managing railway infrastructure, capacity and transport. It also mandates ensuring cyber-security and the resilience of infrastructure.

The Cyber Resilience Act, a proposed regulation concerning cyber-security requirements for products incorporating digital components, strengthens cyber-security regulations to enhance the security of both hardware and software items.

Directive NIS2 should be implemented by EU member states by November 2024. By that time, each entity covered by it should adjust their security

JAKUB TOMCZAK

Jakub Tomczak is a lawyer specialising in railway law, in particular railway safety and interoperability. He has over 12 years of experience working with infrastructure managers, operators and manufacturers. He runs his law firm and an expert blog on railway law in Poland and the European Union.

management systems to the new requirements. The directive imposes the obligation to comply with cyber-security regulations on new entities, including cloud service providers, and introduces the possibility of imposing fines on entities that fail to fulfill their obligations. The cost of fines will depend on the type of entity. For so-called key entities, the fines can go up to 10 million EUR or 2% of the total worldwide turnover in the previous year, while for important entities, they can be up to 7 million EUR or 1.4% of the total worldwide turnover in the previous year, with the higher amount being applied in both cases.

Additionally, the NIS2 Directive introduces new obligations in the field of Cyber-security Management, requiring the mandatory implementation of specific risk management solutions, including policies for risk analysis and security of information systems, incident management policies, continuity of operation plans, and supply chain security.

For this purpose, the cooperation of many entities, including the EU member states themselves, is necessary. Therefore, NIS2 Directive concerning measures for achieving a high common level of cyber-security in the Union has been developed.

Since the railway is facing an inevitable process of digitisation, appropriate measures should be taken to protect it from cybercriminals. Of course, during the production of railway traffic control devices, CENELEC standards such as EN50128 or 50129 apply. However, these are not requirements that would secure the entire railway system.

In summary, the growing importance of cyber-security in the railway sector is undeniable. As the railway becomes an increasingly integrated and digital system, it is essential to take effective protective measures against potential cyber threats. The NIS2 Directive represents a significant step towards securing railway infrastructure and sensitive data. It imposes specific obligations on entities operating in the railway sector, thereby providing a higher level of protection.

It is important to emphasise that cyber-security is not only a technical matter but also requires the cooperation and engagement of all entities, both public and private, within the European Union. Initiatives such as the European Railway-ISAC and standards developed by CENELEC are important tools in building common knowledge and defense measures.

With the process of digitisation, the railway becomes not only a more efficient means of transport but also more vulnerable to attacks. Therefore, it is extremely important to implement new technologies in a secure manner and in accordance with the highest standards.

Looking to the future, a key challenge remains not only maintaining the current level of cyber-security but also swiftly adapting to evolving threats. Implementing new solutions and procedures, monitoring the situation, and continuously improving processes are crucial elements in ensuring the reliability and security of railway infrastructure in the era of digitisation.

@GlobalRailway