JOURNAL OF MODERN SCIENCE

Том 4/53/2023

www.jomswsge.com

DOI: doi.org/10.13166/jms/176679

Alina Paklerska

Alcide De Gasperi University
of Euroregional Economy
in Józefów, Poland

ORCID iD: 0000-0001-7251-9520

CYBER THREATS IN RAIL TRAFFIC IN POLAND

Abstract

A rising network of interconnections, new technologies and an increasing degree of digitization mean that the rail sector, both locally, as well as to a global degree, is currently in the midst of significant internal transformations. Both the business model and infrastructure are being transformed, including that for information systems. The purpose of this analysis is to systemic approach to the subject. Cyber threats are treated here not as a cause of insecurity, but as the result of a system's frailty. The subject of the study is discussed in the context of rail traffic in Poland. The author points out the changes in cyber security that Poland is experiencing and suggests possible scenarios for the near future. He points out that train traffic security is one of the main aspects of the digitization of critical infrastructure in Poland. The author aims to show that train traffic security depends on a number of factors. The article presents a proposed typology of cyber threats to rail traffic.

Keywords: *Poland, internet, cyber security, cyber threats, rail traffic, cyberattack*

In Poland, we can talk about some leading digitization trends in rail transportation (Pieriegud 2019):

- passenger access to the Internet during train travel,
- easy planning of train travel by means of interactive and e-intelligent digital services,
- maintenance, based on continuously transmitted (by electronic systems) data on the wear and tear of individual components of the railroad infrastructure,
- automation and interoperability of traffic control systems, where vehicles are started completely without operational personnel,
- increasing the safety of train traffic.

The first two trends mentioned above are currently being realized in the policies of Polish railroad entities. In principle, in every new passenger train in Poland there is already the possibility to connect to free public WiFi, and passengers can easily plan their trip thanks to a wide range of applications and web portals synchronized with the current train schedule (Cyganek, 2023). However, technologies allowing for e-intelligent control of railroad infrastructure

maintenance and automation of rail traffic control systems have still not been popularized in Poland. Instead, digitalization is currently developing in the latter direction, and to it I would like to devote special attention.

Train traffic safety as one of the aspects of digitization

Train traffic does not have a uniform definition in Polish law. Trains move on railroad lines – designated by the infrastructure manager on railroad roads adapted for train traffic (Railway Transport Law art. 4 pkt 2). The principles of train traffic safety are regulated in state and EU legislation. Train traffic safety refers to one of the tasks of the President of the Railway Transport Authority in the Railway Transport Law. In terms of the European Union's legislation on safety, interoperability and regulation of rail transport, it is the national safety authority and the national regulator of rail transport (Railway Transport Law art. 10 pkt 1). The President of UTK supervises entities whose activities affect the safety of rail traffic. Thus, he controls their compliance with the obligations and criteria necessary for safe operation of the railroad.

Railroad traffic safety depends on a number of factors. In particular on (UTK 2023):

- the technical condition of railroad infrastructure and rolling stock,
- organization of railroad traffic,
- professional qualifications and proper performance of duties by employees.

In the face of developing automation and technological advances, which, according to their purpose, reduce the influence of the technical factor on the occurrence of undesirable events, the focus in the aspect of safety has shifted to the area of human activity and the related human factor. Therefore, the work performed by a person – a driver, a driver of railroad vehicles, or a person working in a railroad position (rozporządzenie o stanowiskach kolejowych), as well as his or her qualifications and mental and physical condition today require special verification. This also became the reason for the establishment

on January 1, 2023 of a state-of-the-art government application covering human resources issues in rail traffic located at www.maszynista.gov.pl (Register of Train Drivers and Train Drivers). This is a database of all train drivers in Poland. The maintenance of this register involves the addition of data to it by railroad market players and the drivers themselves. This is the largest project in several years to maintain safety in the rail sector in Poland.

However, it is not the only example of the expansion of new technologies into the sphere of railroad safety. In the aspect of protection and monitoring of railroad infrastructure, the innovative project was undertaken by the US. *The carriers there, which are also railroad managers, use Railway Daily Operations Control Systems (RailDOCS). This is a system that manages the process of diagnostics and maintenance of railroad lines. It relies on the fact that all the key elements that make up the rail network, turnouts, crossings, signaling devices, traffic lights or lighting have been cataloged and entered into the system's server memory. It later manages their maintenance by reminding them of periodic diagnostics. The employee is equipped with a mobile terminal, on which he list the elements of a given facility, which he then inspects. The effect of his work is sent to the main server where it is processed* (Kurier Kolejowy 2023). Hamburg, meanwhile, introduced a controlled digital light rail in 2022. *The trains run largely autonomously, with the driver or engineer intervening only in case of disruptions. There are plans to use the system on other routes, and the Hamburg model could serve as a model for similar projects in other cities* (Deutschland 2022).

Cyber threats to rail traffic

According to numerous opinions of rail market experts, as well as the voices of representatives of the Polish and EU administrations in Poland in the 2020s, the most relevant aspect in the railroad IT space will be security. Railroad cyber-security interacts with safety in rail traffic. In other words, secure information systems that support rail traffic contribute to its overall safety.

Railroads belong to a strategic sector for state economies. Therefore, rail traffic safety is not only important for passengers using the services of rail carriers. Any possible threats also affect the stability of individual countries.

So far in Poland, the rail sector has not been a direct target of cyber attacks, but several more serious incidents have already been reported, showing the vulnerability of the sector, including the most notorious one on March 17, 2022, when the equipment of 19 of 33 Local Traffic Control Centers crashed (PAP 2022). The damage to these devices resulted in a state where rail connections could not be safely managed.

However, it should be assumed that cyber attacks, such as the one that occurred in Italy six days after the aforementioned incident, may also occur in the near future. *On Wednesday, March 23, there was a cyber attack on Italy's state-owned rail operator, Ferrovie dello Stato Italiane (FS). An intrusion was detected in the IT systems of two FS subsidiaries – Trenitalia (responsible for train operations) and Rete Ferroviaria Italiana (manager of Italian railroads). In order to thoroughly check the systems and fix the glitches, FS precautionarily suspended ticket sales at its ticket offices and from ticket machines at train stations, while online sales operated normally. There are many indications that this was a ransomware attack, nevertheless there is no information on the possible effects on the company or whether any data was stolen. (…) The Italian news agency ANSA suggested that the cyber attack in Italy was carried out by a Russian hacking group* (Przasnyski 2022).

On July 9, 2021, there was a cyber attack on Iran's railroads. It caused suspensions, delays and cancellations, as well as false announcements on station information boards. The latter spoke of long delays caused by the cyber attacks. They suggested that passengers call Ayatollah Ali Khamenei's office about problems, quoting his number. The ticketing system was also damaged, resulting in passengers being unable to enter platforms, causing chaos at stations.

According to Article 2(4) of the (Ustawa o krajowym systemie cyberbezpieczeństwa) *Cyber-security is the resilience of information systems against actions that compromise the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems*. This definition does not so much imply actions to prevent cyber attacks as to repel them and not allow them to cause damage.

In light of the increasing frequency of cyberattacks on rail infrastructure, it is important to look for the source of these threats. Konrad Snopkiewicz

points to three types of cyber threats, dividing them into three groups (Snopkiewicz 2020):

I. **group addictive** – Dangers caused by the *human factor* (improper operation of equipment by humans, negligence, inadequate communication between operating personnel);
II. **hardware group** – dangers caused by the use of underdeveloped software or faulty equipment in professional work;
III. **criminal group** – threats caused by the exploitation of the aforementioned errors, omissions and vulnerabilities by criminals and cyber-terrorists.

Cyber threats are an inherent property of any system. They arise where we have to deal with:

- a defect in the hardware or software supporting the work of personnel;
- failure to prepare adequate safeguards against attacks;
- faulty work of personnel.

Protection of the system should therefore not only have a technical dimension, and the reasons for vulnerability to cyber threats should be found in the inadequate management of the enterprise.

Technically advanced solutions entail ever-increasing demands on personnel. Employees should therefore have the appropriate competencies expressed in (Barge, Morreale 2007):

- knowledge of procedures resulting from proper preparation for their work,
- the skills necessary to perform the tasks of their positions,
- motivation to constantly improve their qualifications in order to professionally perform the tasks assigned by the employer.

Therefore, it is necessary not so much to combat the effects of undesirable incidents, but to learn about their causes and introduce appropriate countermeasures to offset the risks.

Typology of cyber threats to rail traffic

A sui generis threat means the possibility of an undesirable condition, event or occurrence of a fact that may cause negative consequences for the subject of the threat. It creates a sense of insecurity (Lubiewsk, Dróżdż 2020).

With regard to rail traffic, the subjects of these risks are the most important elements of the rail system, namely equipment, infrastructure, service providers and service recipients. Three elements are therefore singled out that require adequate protection against the occurrence of undesirable events.

The first consists of railroad vehicles and technical elements indicated in Annex 1 of the Railway Transport Law, including railroad tracks, facilities located on the trackside, platforms and lighting systems for maintaining safety in train traffic.

As the second area, the service provider is indicated, by which is meant not the company, which is made up of the people working in it. For the purposes of this article, I would like the company's personnel to be understood more broadly than the definition of railroad personnel adopted in Polish law indicates (rozporządzenie o stanowiskach kolejowych § 2 pkt 4). These will be all those who have a direct and indirect impact on rail traffic safety, that is, all employees of railroad entities, regardless of their profession or position.

The third element of the railroad system is the service recipients. The largest *customers* of railroad entities are usually states. In addition, the entities are service providers in the passenger and freight sectors, so their customers are individuals and businesses.

Each of these three elements of the rail traffic system is the subject of defensive actions against cyber threats. Preventive measures, such as raising the competence and motivation of personnel, for example, can contribute to more effective protection against the effects of undesirable events.

Reiterating the conclusion regarding the causes of cyber threats, they can therefore be divided into two groups. The first relates to internal system problems, including errors on the part of personnel, misuse by service recipients, or malfunctioning equipment.

In contrast, the second group of cyber threats, which have external sources, includes hacktivism, cyberterrorism, cybercrime and cyberattacks. The

indicated types of external threats essentially differ only in the goal that the senders of the activities indicated above want to achieve, but the methods used in them are the same (e.g. viruses, bacteria, worms, logic bombs, Trojan horses, spoofing, sniffing, DoS, or DDoS).

Afterword

Faced with a major technological change, on December 14, 2022. The European Parliament and the Council adopted the NIS 2 Directive, which includes the rail transport sector as a key player and requires it to ensure:

- risk analysis and information systems security policy,
- incident handling (prevention, detection and response to incidents),
- business continuity and crisis management,
- supply chain security,
- security in the acquisition, development and maintenance of networks and information systems (including handling and disclosure of vulnerabilities),
- procedures (testing and auditing) to assess the effectiveness of cyber security risk management measures,
- use of cryptography and encryption.

There are two years for transposition to apply in accordance with the regulations. By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive – we read in the NIS 2 Directive. Member states, according to the directive, will adopt national strategies cyber security that will provide for strategic objectives, resources key to achieving these objectives, and appropriate measures of public policies and regulations, with a view to achieving and maintaining a a high level of cyber security.

The directive points to the need to extend the application of cyber security regulations to a larger part of the economy in order to „ensure comprehensive coverage of sectors and services that are essential for key social and economic activities social and economic activities in the internal market.

In conclusion, it should be pointed out that activities, as well as the perception itself of the need to strengthen cyber security in the rail sector, are evolving slowly. Many issues, such as those concerning motivation and procedures at the personnel level (such as drivers' working hours) still need to be analyzed at the legal level.

In addition, also noteworthy is the need for a holistic approach in protecting against cyber threats, one in which the company would take preventive measures covering all elements of the rail system, which would result in reducing the scope of the effects of undesirable events in the future.

References

Barge, J. K., Morreale S. P. i inni. (2007). Komunikacja między ludźmi. Motywacja, wiedza i umiejętności.

Bezpieczeństwo i nadzór. https://utk.gov.pl/pl/bezpieczenstwo-systemy/14722,Bezpieczenstwo-i-nadzor.html [dostęp 18.08.2023].

Bezpłatne Wi-Fi we wszystkich pociągach EIC PKP Intercity. https://www.intercity.pl/pl/site/o-nas/dzial-prasowy/aktualnosci/bezplatne-wi-fi-we-wszystkich-pociagach-eic-pkp-intercity.html [dostęp 18.08.2023].

Cyberatak na irańskie koleje. https://www.altair.com.pl/news/view?news_id=34081.

Cyberbezpieczeństwo kluczowe dla bezpiecznej kolei. Dostęp 18.08.2023 z https://utk.gov.pl/pl/aktualnosci/20101,Cyberbezpieczenstwo-kluczowe-dla-bezpiecznej-kolei.html dostęp [18.08.2023].

Cyfrowe pociągi i inteligentne systemy planowania tras. https://www.deutschland.de/pl/topic/gospodarka/mobilnosc-przyszlosci-rozwiazania-cyfrowe-z-niemiec

Cyganek, A. (2023). 10 aplikacji które warto mieć podróżując koleją, autobusem lub taksówką. https://www.gsmmaniak.pl/636056/10-aplikacji-transport/ [dostęp 18.08.2023].

Czynniki ludzkie i organizacyjne – Kryteria SMS. https://utk.gov.pl/pl/bezpieczenstwo-systemy/zarzadzanie-bezpieczen/wspolne-metody-bezpiecz/kryteria-sms/19149,Czynniki-ludzkie-i-organizacyjne.html [dostęp 18.08.2023].

Lubiewski, P., Dróżdż. A. (2020). Zagrożenie – rozważania na gruncie teorii. http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-9c41d4a4-df15-4350-9bc2-c41027ea0d1e. 1(34). Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy [dostęp 18.08.2023].

Nowe technologie dbają o bezpieczeństwo na kolei. https://kurier-kolejowy.pl/aktualnosci/18322/nowe-technologie-dbaja-o-bezpieczenstwo-na-kolei.html [dostęp 18.08.2023].
Pieriegud, J. (2019). Transformacja Cyfrowa Kolei. https://assets.new.siemens.com/siemens/assets/api/uuid:54cbf7fb-04a6-4a95-8d5d-62fd9c921d25/cyfrowa-transformacja-kolei-raport-sgh.pdf [dostęp 18.08.2023].
Przasnyski, F. (2023). Cyberatak we Włoszech uderzył w kolej i spowodował znaczne opóźnienia. https://obserwatorlogistyczny.pl/2022/03/28/cyberatak-we-wloszech-uderzyl-w-kolej-i-spowodowal-znaczne-opoznienia/ [dostęp 18.08.2023].
Snopkiewicz, K. (2020). Przegląd zagrożeń w cyberprzestrzeni, 2020/9, s. 34. Studia Administracji i Bezpieczeństwa.
Ziemska, A., Oksiuta, A. i inni. (2023). Ogólnopolska awaria na kolei. Podano przyczynę. https://www.pap.pl/aktualnosci/news%2C1118022%2Cpotezna-awaria-na-kolei-duze-opoznienia-odwolane-pociagi.html [dostęp 18.08.2023].

Law Acts

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)
Rozporządzenie Ministra Infrastruktury z dnia 11 stycznia 2021 r. w sprawie pracowników zatrudnionych na stanowiskach bezpośrednio związanych z prowadzeniem i bezpieczeństwem ruchu kolejowego oraz prowadzeniem określonych rodzajów pojazdów kolejowych, Dz.U.2021.101.
Rozporządzenie Ministra Infrastruktury z dnia 18 lipca 2005 r. w sprawie ogólnych warunków prowadzenia ruchu kolejowego i sygnalizacji, Dz.U.2019.2352.
Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym, Dz. U.2023.789, test jednolity.
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U.2022.2666, tekst jednolity.