ORIGINAL ARTICLE
DOI: https://doi.org/10.30932/1992-3252-2023-21-6-12

World of Transport and Transportation, 2023,
Vol. 21, Iss. 6 (109), pp. 268–274

Transport Cybersecurity

Evgeny A. NESTEROV **Viktor Ya. TSVETKOV**

Evgeny A. Nesterov[1], Viktor Ya. Tsvetkov[2]

[1, 2] Russian University of Transport, Moscow, Russia.
[1] ORCID 0009-0009-9100-3410; Web of Science Researcher ID: JUF-4957-2023; Scopus Author ID: 58707809100; Russian Science Citation Index SPIN-code: 9008-0780, Russian Science Citation Index Author ID: 1119794.
[2] ORCID 0000-0003-1359-9799; Web of Science Researcher ID:) J-5446-2013; Scopus Author ID: 000313599799; Russian Science Citation Index Author ID: 1399061.
✉ *[2] cvj2@mail.ru.*

ABSTRACT

A feature of the digital transformation of the transport industry is the trend to increased number of cyberattacks that are among the information threats. Transport cybersecurity is a broader phenomenon compared to cyberattacks and information security. It includes organisational security and other types of security that are not found purely in the information field.

The relevance of transport cybersecurity is additionally due to the widespread use of information and computer networks and information space. Cyberspace in the transport sector can be interpreted as an aggregate of networks, information space, communication and real environment. The inclusion of real environment in transport cyberspace is a distinctive feature of transport cyberspace.

The growth of information threats occurs regardless of development of transport cyberspace. It is due to digitalisation of society, including the transport sector. Cyberspace creates the preconditions for cyberthreats of a new quality, and for new cyberthreats, previous methods of information security become ineffective. The emergence of information threats is dictated not so much by digitalisation, but rather by the openness of information and communication technology. Multimodal transportation as a relationship between many organisations also contributes to the growth of cyberthreats and a decrease in information security.

The article provides an analysis of the state and approaches used in transport cybersecurity based on the review of publications on the topic, suggests a taxonomy of threats and risks to transport cybersecurity, introduces the concepts of «railway information» and «transport information», describes the vulnerabilities of transport cyberspace.

Keywords: transport, transport cyberspace, transport cybersecurity, cyber-physical systems, network systems, digital risks, cyber-physical threats.

For citation: Nesterov, E. A., Tsvetkov, V. Ya. Transport Cybersecurity. World of Transport and Transportation, 2023, Vol. 21, Iss. 6 (109), pp. 268–274. DOI: https://doi.org/10.30932/1992-3252-2023-21-6-12.

The text of the article originally written in Russian is published in the first part of the issue.
Текст статьи на русском языке публикуется в первой части данного выпуска.

INTRODUCTION

Digitalisation is transforming railways around the world. One of the features of digital transformation of any industry, including railways, is increased susceptibility to cyberattacks [1–3]. The railway industry is vulnerable to such attacks because of the growing number of digital elements, as well as of interfaces between digital and physical components in railway systems. The increase in the number of elements and interfaces requires new structures, concepts and architectures to ensure the resilience of the railway system to cybersecurity challenges such as lack of proactiveness, lack of a holistic approach and aging security systems exposed to future cyberthreats.

Railway transport is an important industry. Currently, in the field of transport, there is cyberspace as an industrial cluster, including integration of information systems, intelligent transport systems, Internet of Things technology, transport cyber-physical systems, telecommunication networks, digital railway [4] and so on. A transport cybersecurity breach can create many critical situations. Modern transport systems do not operate in isolation but use different networks to improve business processes. These developments have as consequences an increased exposure to cyber threats.

The *objective* of the study offered in the article was the analysis of the state of transport cybersecurity and of the applied approaches, described in research papers, of taxonomy of threats and risks to transport cybersecurity, of vulnerabilities f transport cyberspace.

RESULTS

Causes of Cyberthreats

Railway cyberspace includes communication lines and access points, as well as transport control points. Corporate business is widely practiced in railway transport. This is especially noticeable in multimodal transportation. Many organisations and individuals are involved in this business. Many participants in a corporate business create multiple connections in which there are many access points. Connections grow in cubic progression. Connections and access points create the opportunity for unauthorised persons to access cyberspace, that is, it creates cyberthreats. These threats should be classified as external threats.

In addition, a large number of different software programs operate in cyberspace, which are not always properly coordinated. Software mismatch creates additional threats proportional to the size of the network in cyberspace. The specifics of communications in transport require the introduction of the concept of «transport information». In the field of railway transport, transport information (TI) becomes railway information (RI). This information is divided into control and descriptive RI. Unauthorised access to any of this information poses a threat.

An additional source of cyberthreats are organisational or regulatory threats. Many regulatory documents of different industries and organisations are not fully harmonised. Mismatch of regulatory documentation serves as a source of internal threats to functioning of the transport system. The peculiarity of TI and RI is that they are organised into blocks that have the property of integrity and consistency. Possible violation of information integrity also poses a threat. Thus, regulations, communication lines, access points, and information blocks create external and internal cyberthreats.

Railway infrastructure is increasingly moving towards smart and cyber-physical systems, which creates new risks and opportunities for cybercrime.

There are problems in operation of transport infrastructure, problems referring to Big data [5] have their own specifics regarding railways [6], law on transport cybersecurity is missing.

Measures to counteract cyberattacks on railway transport are under development. There is an ongoing process of systematising the risks and their consequences that should be avoided. For instance, these risks are systematised in [7]. From the standpoint of categorical analysis, the concept of risk category or risk categories can be introduced. Risk categories comprise traffic delays; «anthropoentropy»; collisions; track damage; acts of terrorism; human casualties; man-made factors; loss of competitiveness; leakage of valuable information.

Abnormal situations periodically occur at transport infrastructure facilities, some of which are described in [1]. These cases are due to development of IT technologies and to a possibility of intentional or unintentional access to communication channels and of interference in transport control channels.

At the same time, access to confidential information can be not only direct, but also indirect. For example, information transmitted by email is open at no less than seven points at

different transmission nodes. Here we should note such a threat as the transfer of proprietary information or information about proprietary information in personal email messages. To prevent this threat, for example, in the UK it is prohibited to use business email to transmit personal information or to private addresses of individuals.

Shift2Rail.

The study [8] examined several European projects, devoted to cybersecurity, from the perspective of Shift2Rail.

In the framework of five phases of Shift2Rail project, several work packages have been implemented (IP2 Technical Demonstrators. Advanced Traffic Management and Control Systems [1]), the fifth phase been finalised in October 2023.

To improve the security of the cyberspace, standardisation methods and ISO standards are also used. The standardisation method and standards are divided into four groups: international, national, industry and within a specific enterprise.

Dominants in Cybersecurity

Among many security technologies for the cyberspace of transport infrastructure, based on analysis and generalisation, the dominant or most important technologies for the transport industry were identified [10]. These technologies are called security dominants. Among them, we should highlight standard ones, such as access control, and special ones, such as reduction of entry points. In addition, we can note cognitive information technologies such as «handshake» technology, unified security centre technology, etc. [11].

Access control security

Access control security is a fundamental issue for ensuring the security of any control system or technical system. A typical approach to implementing access is to use an access control list (ACL), role-based access control (RBAC) [12], task-based access control (TBAC) [13]. Access control technologies are divided into four categories: team-based (TMAC), spatial [14], cognitive (CAC), context-based (CBAC) [15] access control. Spatial control is associated with actions in real space and requires organisation of physical protection. TMAC requires communication, information and cryptographic protection. Cognitive access control requires the analysis of cognitive models and the use of cognitive logic. Context-based access control requires the use of semantic analysis and latent analysis of transmitted TI and RI. In addition, for security purposes, client identity authentication, single sign-on methodology, etc. are used. Requirements for access control are summarised in [16].

One method is to use a safe data list. An incorrect safe list creates incorrect access control. This can lead to dangerous scenarios where incorrect data can be used to weaken the security of the infrastructure.

Security of Information Transmission

An important factor in cyberspace is the security of information transmission. Enterprise Service Bus (ESB) technology is used to understand multiple systems sharing data and services on a railway information exchange platform.

Security of Information and Resource Storage

Ensuring reliable storage of information, models and resources is an important task for the security of RI and TI. Databases are a weak link in this problem because they widely use standard query and search methods, and most importantly, standard and simple data structures. Databases are focused on simplicity and accessibility, while security technologies require access restrictions and unique forms of stored information. Cloud processing and cloud storage partially solve this problem. However, the use of cloud and fog technologies complicates the information management structure. This entails an increase in threats to cybersecurity in information management technologies. Simple control technology carries less risk. Complex information management technology carries greater risks and a greater number of emergency situations. The problem is also solved by the technology of specialised data warehouses.

Security management centre **[11]**

These functions are performed by situation centres. Centralisation of security management is an effective organisational measure that eliminates minor and accidental penetrations of

[1] [Electronic resource]: https://projects.shift2rail.org/s2r_ip_TD_r.aspx?ip=2&td=1bccaf76–7915–4283–8b52–36afdb1bdf42.

confidential information. Situation centres create a single protection system and an easily manageable security system. They allow accumulating experience of threats and penetration attempts. On this basis, with involvement of intelligent systems such as artificial neural networks, unique protection systems are created for each transport infrastructure facility. A centralised security system creates an internal cyberspace security system as a self-organising system. This is very important against the backdrop of constantly growing and changing external threats.

Cybersecurity Threats to Railways

There are several threats associated with railway cybersecurity. The predominant operational challenge for the railway sector is threats to identity, privacy and data systems. The most important ones should be highlighted [2].

Motivated Risks and Threats

This class of threats is not aimed at destroying, damaging or stealing information, but at damaging the reputation of an organisation, corporation, intermediary company, or government. The main reason for a motivated attack on the system is competition, which is aimed at loss of clientele and subsequent damage.

Quite often, these threats use an «agent-based» approach that uses individual and group algorithms. An agent, like a virus, can adapt to its environment and has polyformity, that is, the ability to change shape when detected. This type of threat is also called «political».

Pragmatic Threats

They involve the use of intermediaries and third parties who may have financial information or information about financial information or information about persons with access to financial information.

Communication threats

They are associated with the weakness of communications and the presence of weak points in them. They include not only the theft of information, but also damage to information and even its substitution to harm technology and transportation.

Data Retrieval

This threat involves the use of attributes of IT technologies for the subsequent illegal use of already important information. This data may be subject to bargaining or blackmail.

Database Threats

A database is an information storage system and an information processing system. Initially, DB were created for a wide range of consumers and their concept was and remains ease of use. There are standard or generic database formats, which greatly simplify access to such systems. A method of protection can be storing data in a DB not in a «pure»

form, but in the form of fragments of structures or in encoded form.

Mirroring and Redundancy

These technologies are neighbouring but have differences. When mirroring, information and information images or clusters are practically cloned. When making a backup (which is also based on copying), it is possible to exclude unimportant information to save physical memory. The weak point of both technologies is that mirrors and backups are not stored with the same care as the original. The security system for copies is usually much weaker than for the original information. Therefore, it is recommended to maintain the same security policy for copies as for the originals.

Server Threats

It is customary to divide servers into main ones and application servers. It is common practice to protect core servers more carefully than application servers. The danger is that through a weakly protected application server it becomes possible to access the main server with valuable information.

Administrators' Threats

This specific type of threat is man-made and is based on the psychological characteristics of any person, which includes a system administrator. Because of this, the type of threats has got this name. The threat is implemented through communication between an attacker and a system administrator under conditions of information uncertainty. The attacker impersonates another person and, in the end, receives a fragment or all the necessary information to enter the protected system. This entry mechanism is acceptable for any security system employee. But administrators represent the greatest information value.

A threat closely related to this one is «emergency» entry. In case of a failure or power failure of the information system, the security system is disabled for seconds. This is enough for attackers to penetrate the system and then log in after the failure is eliminated.

System Violation

The consistency of data and processing algorithms includes completeness, integrity, structure, and complementarity. Security systems prioritise privacy. Secondly, an integrity analysis is carried out. As for data modification, this is the third priority task. One of the security tools in this part is logging. But it records events, leaving the content of events without attention. It can be noted that many algorithms are an analogue of the system. Many algorithms are modelled after prototype algorithms. Knowing the prototype of an algorithm gives knowledge about the modified algorithm and gives knowledge to modify the current algorithm.

It refers to data as well. Their formats and structure are based on prototypes. Knowing the prototype structure provides knowledge about the current data structure. Thus, modification of the algorithm and modification of the data format entail destructive consequences.

For security systems and the systems they protect, there are a large number of attacks, which are divided into distributed, cognitive and targeted (vector) ones. Systems for repelling attacks are arranged commensurately.

There are groups of stochastic threats. They are most often associated with the influence of the external environment and the stochasticity of the operating environment of the control system or controlled transport system.

Insider threats are similar to malicious acts, but come from within the organisation.

Cybersecurity of Transport Cyber-Physical Systems

Cyber-physical systems comprise among others transport cyber-physical systems (TCPS) [18]. These systems replace ITS and serve as the basis for digital transport management. The increasing use of TCPS to connect various components of the rail industry and increased connectivity through communications technologies have also led to cyberthreats against TCPS. TCPS implementations require that risks be proactively identified, clearly defined, and secured. To improve operational safety and efficiency, an increasing number of physical railway components are connected through various TCPSs via communications, creating a new paradigm of the «Railway Internet of Things». The trend towards TCPS integration has also led to the ever-increasing dependence of the railway industry on cyber- and IoT technologies, which increases the dangers of cyberthreats. The railway industry is exposed to cyber risks inherent in TCPS deployments. Unfortunately, TCPS components provide not only the desired connection, but also opportunities

Table 1

TCPS Threat Taxonomy

Parts of railway cyber-physical system	Possible threats
New generation train control systems (for example, ERTMS, ETCS, PTC, CBTC)	Multiple attacks including electromagnetic interference, jamming, denial of service (DoS), message modification and unauthorised access, etc.
	Brute force attacks, unauthorised network access and message modification
	Passive eavesdropping, active relinquishment of control and taking control
Traditional railway signalling systems	Unauthorised network access, denial of service (DoS) and message modification
	Electromagnetic interference
Balise data transfer	Violation of availability or integrity of data balises [eurobalises], jamming, electromagnetic interference
Railway traction divisions, electric power supply systems	False data injection attacks, message modification and unauthorised network access
Human-machine interface	Multiple attacks including denial of service, message modification, unauthorised access, etc.
Public address (PA) or public information display systems	Unauthorised intrusions
Railway track infrastructure	Both physical and cyber intrusion

for attackers to achieve malicious goals. Table 1 [19] provides a taxonomy of threats to TCPS.

Common cyber technologies [19] are frequently used across industries, and their underlying security designs are well understood through technical iterations and IT research.

CONCLUSION

Cyberspace is interpreted in a narrow and broad sense. In a narrow sense, this is the information space of digital twins and cyber-physical systems, the information space of unmanned vehicles, as well as Internet of Things technology. In a broad sense, cyberspace includes the open networks, and all means of communication associated with management of transport systems, information systems and intelligent systems. For all types of these spaces, there are cyberthreats or threats in cyberspace.

There are several reasons for the rise in cyberthreats. The first reason is the growth of open networks and systems.

The second reason is globalisation, which increases society's access to technologies and systems.

The third reason is convergence or universalisation. Universal remote controls are produced that control the TV and the vehicle. Smartphones are produced that can not only make telephone calls, but also control the TV and create interference or control a vehicle.

The fourth reason is the increase in volumes of information, which provokes a person to have the opposite reaction to simplify information. The growing volume of information is not accompanied by the growth of the use and sophistication of passwords as means of protection. It becomes easier for everyone to crack passwords using stereotypes.

The fifth reason is the growing complexity of technical and information systems. This growth also creates a trend towards making such systems easier to work with. Simplifying work entails reducing information security.

The sixth reason is the growth of information asymmetry between the requirements of technical and information systems and the real ability of a person to manage these systems. There is an advance in the growth of the complexity of systems in relation to the growth of the abilities and capabilities of the human manager.

The seventh reason is the growing digital inequality[2]. This is the inequality in IT skills between countries and between people. Some advanced IT specialists oppose themselves to society and commit destructive actions to demonstrate superiority. The digital divide is growing in the «leader–performer» system. As a rule, a manager understands less about IT technologies than an ordinary employee and even less than an expert. This misunderstanding is expressed in the inhibition of innovative IT developments. Such a manager gives preference to simple, but more understandable security

[2] See, e.g., DiMaggio, P., Hargittai, E. From the 'Digital Divide' to 'Digital Inequality': Studying Internet Use as Penetration Increases. Princeton University, Woodrow Wilson School of Public and International Affairs, Center for Arts and Cultural Policy Studies, Working Papers. 2001.

systems, without paying attention to their weak security. Such a leader rejects complex and incomprehensible to him, but well-protecting security systems.

The eighth reason is the emergence of cyberspace as a tool for managing an open system.

The ninth reason for the growth of cyberthreats is due to the use of large networks, most of which are open.

There is a growing tendency to differentiate cybersecurity research, rather than writing a general theory. The need to develop an integrated framework for solving many cybersecurity problems remains urgent. Analysis [2] shows that most cybersecurity research conducted on railways is still conceptual in nature and lags in the application of artificial intelligence (AI)-based security. As in other industries, it is very important that railways also follow the latest security technologies,

REFERENCES

1. Thaduri, A., Aljumaili, M., Kour, R., Karim, R. Cybersecurity for eMaintenance in railway infrastructure: risks and consequences. *International Journal of System Assurance Engineering and Management*, 2019, Vol. 10, Iss. 6, pp. 149–159. DOI: 10.1007/s13198-019-00778-w.

2. Kour, R., Thaduri, A., Karim, R. A review on cybersecurity in railways. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, 2023, Vol. 237, Iss. 1, pp. 3–20. DOI: 10.1177/09544097221089389.

3. Wang, Z., Liu, X. Cyber security of railway cyber-physical system (CPS) – A risk management methodology. *Communications in Transportation Research*, 2022, Vol. 2, Iss. 4, 100078. https://doi.org/10.1016/j.commtr.2022.100078.

4. Lyovin, B. A., Tsvetkov, V. Ya. Digital Railway: Principles and Technologies. *World of Transport and Transportation*, 2018, Vol. 16, Iss. 3 (76), pp. 50–61. DOI: https://doi.org/10.30932/1992-3252-2018-16-3-5.

5. Lyovin, B. A., Tsvetkov, V. Ya. Information Processes in Big Data Environment. *World of Transport and Transportation*, 2017, Vol. 15, Iss. 6 (73), pp. 20–30. DOI: https://doi.org/10.30932/1992-3252-2017-15-6-2.

6. Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., Khan, S. U. The rise of «big data» on cloud computing: review and open research issues. *Information Systems Journal*, 2015, Vol. 47, pp. 98–115. DOI: 10.1016/J.IS.2014.07.006.

7. Bloomfield, R., Bendele, M., Bishop, P., Stroud, R., Tonks, S. The Risk Assessment of ERTMS-based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned. In: International Conference on Reliability, Safety and Security of Railway Systems. Springer, 2016, pp 3–19. DOI: 10.1007/978-3-319-33951-1_1.

8. Masson, É., Gransart, C. Cyber Security for Railways – A Huge Challenge – Shift2Rail Perspective. In: International workshop on communication technologies for vehicles. Springer, Cham, 2017, Vol. 10222, pp. 97–104. DOI: https://doi.org/10.1007/978-3-319-56880-5_10 [restricted access].

9. Álvarez, A., Ioannidis, S., Schlehuber, C., Rodríguez, F., Vallero, V. CIPSEC Project [Online]. 2017. [Electronic resource]: https://upcommons.upc.edu/handle/2117/106378. Last accessed 14.11.2023.

10. Cao, N., Wang, C., Li, M., Ren, K., Lou, W. Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data. *IEEE Transactions on Parallel and Distributed Systems*, 2014, Vol. 25, Iss. 1, pp. 222–233. DOI: 10.1109/TPDS.2013.45.

11. Shi, H. Railway Information Sharing Platform Security Requirements Analysis. In: ICLEM 2014: System Planning, Supply Chain Management, and Safety. 2014, pp 1116–1121. DOI: https://doi.org/10.1061/9780784413753.169.

12. Edwards, W. K. Policies and Roles in Collaborative Applications. In: Proceedings of the 1996 ACM conference on Computer supported cooperative work 1996. ACM, pp 11–20. [Electronic resource]: https://faculty.cc.gatech.edu/~keith/pubs/policy.pdf. Last accessed 14.11.2023.

13. Thomas, R. K., Sandhu, R. S. Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management. Database security XI. Springer, Berlin, 1998, pp 166–181. DOI: 10.1007/978-0-387-35285-5_10.

14. Bullock, A. SPACE: spatial access control for collaborative virtual environments. Doctoral dissertation, University of Nottingham, 1999. 183 p. [Electronic resource]: http://www.adrianbullock.com/documents/thesis.pdf. Last accessed 14.11.2023.

15. Covington, M. J., Long, W., Srinivasan, S., DEV, A. K., Ahamad, M., Abowd, G. D. Securing Context-Aware Applications Using Environment Roles. In: Proceedings of the sixth ACM symposium on access control models and technologies 2001. ACM, pp 10–20. DOI: https://doi.org/10.1145/373256.373258 [restricted access].

16. Tolone, W., Ahn, G., Pai, T., Hong, S. Access Control in Collaborative Systems. ACM Computing Surveys (CSUR), 2005, Vol. 37, Iss. 1, pp. 29–41. DOI: 10.1145/1057977.1057979.

17. ENISA (2015) Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations, European Union Agency for Network and Information Security. [Electronic resource]: https://www.enisa.europa.eu/publications/good-practices-recommendations. Last accessed 14.11.2023.

18. Tsetkov, V. Ya. Control using cyber-physical systems [*Upravlenie s primeneniem kiber-fizicheskikh sistem*]. *Perspectives of science and education*, 2017, Iss. 3 (27), pp. 55–60. [Electronic resource]: https://pnojournal.files.wordpress.com/2017/04/pdf_170310.pdf. Last accessed 14.11.2023.

19. Knowles, W., Prince, D., Hutchison, D. [*et al*]. A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, 2015, Vol. 9, pp. 52–80. DOI: 10.1016/j.ijcip.2015.02.002 [restricted access]. ●

Information about the authors:

Nesterov, Evgeny A., *Ph.D. (Law), Associate Professor, Director of the Law Institute of Russian University of Transport, Moscow, Russia, jnesterov@yandex.ru.*

Tsvetkov, Viktor Ya., *D.Sc. (Eng), Professor, Deputy Director of the Law Institute of Russian University of Transport, Moscow, Russia, cvj2@mail.ru.*

Article received 22.09.2023, approved 19.12.2023, accepted 23.12.2023.