DOI 10.5817/MUJLT2022-1-1

INSURANCE OF CYBER RISKS IN INTERNATIONAL TRANSPORT

by

PETR DOBIÁŠ*

The international transport of goods, passengers and luggage is recently facing the threat of cyberattacks. The article is focused on the analysis of the possible cyber risks in the field of the international transport and their management created by the international governmental and non-governmental organisations. The international regulation of the cybersecurity has only recommendatory character and will be subject to future development. That's the reason why should carriers pay greater attention to all possible cyber security measures. As the instrument of the reduction and mitigation of cyber risks could be used cyber-insurance. The insurance companies are offering insurance cover mainly on individual base corresponding to the extent of protection required by the policyholder.

KEY WORDS

Contractual Conditions, Cybersecurity, Insurance, Insurer, International Transport, Mitigation, Risk

1. INTRODUCTION

The technological progress in the field of management and operation of international transport of passengers and goods goes hand in hand with the implementation of the new advanced computer systems. The analysis provided in this article will be focused on the high technologies designed for the maintenance and operation of traffic systems used in the transport of goods, persons and their luggage. The significance of the analysis is underlined by the recent development in the field of maritime transport.

* E-mail: petr.dobias@vsci.cz, Assistant professor, CEVRO Institut, Chair of Private Law, Prague, Czech Republic.

The Maersk automated terminals were under cyber attacks[1] conducted by anonymous hackers in 2017,[2] which caused malfunction of the loading platforms at the port of discharge and led necessarily to the manual operation of the loading devices. Not only the landing ports, but also sea going vessels are not adequately protected against cyber-attack, because their operating systems are often old fashioned: the navigation software is subject the updates usually only during the necessary maintenance works or within the modernisation of the on-board navigation systems.

The navigation systems of the ships are on one hand well designed for the accident prevention, but on the other hand are also vulnerable to the security violation, because of the missing firewalls and other security features. The dual control systems and back up files are components of the most up-to-date operating systems only, which are present on the board of the sophisticated container vessels and ocean liners.

The malfunction of the GPS navigation systems and data corruption of the Electronic Chart Display and Information Systems (ECDIS) are usually excluded from the insurance cover. The target of a cyber attack could be also the largest maritime cargo vessel, the HMM Algericas, which can carry up to 23,964 containers (TEUs) at a time and cost over USD 140 million[3]. The vulnerability of the navigation systems could theoretically lead to the remote control of twelve naval vessels of this class in the property of HHM (formerly known as Hyundai Merchant Marine), each weighing 215,000 tonnes and measuring 399,9 meters in length.

It should be mentioned, that operators providing intelligent public transport services don't spend sufficient financial sources on development,[4] security and maintenance of security systems.[5] For that reason are state departments and agencies adopting measures for mitigation, planning and

---

1 Cyber attack is defined as "*attack on IT infrastructure in order to cause damage, or to obtain sensitive or strategically important information*" (Jirásek, P., Novák, L., Požár, J. (2015) *Výkladový slovník Kybernetické bezpečnosti*, Prague: PA CR in Prague, Czech branch of AFCEA, p. 71).

2 Saul, J. (2017): *Global shipping feels fallout from Maersk cyber attack*. [online] Thomson Reuters. Available from: https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE/ [Accessed 1 January 2021].

3 Author not specified. *Say hello to HMM Algericas, the largest container vessel on earth* , [online] Shipping and Freight Resource. Available from: https://www.shippingandfreightresource.com/hmm-algericas-largest-container-vessel-on earth [Accessed 15 October 2021].

4 Innovative approaches to ITS security (blockchain, anonymous authentication in fog, bloom filter, security by contract and sensor fusion) are specified e.g. in Mecheva, T., Kanakov, N. (2020) Cybersecurity in Intelligent Transportation Systems, *Computers*, 9, 83, p. 6-8 [online]. Available from: www.mdpi.com/journal/computers [Accessed 10 November 2021].

monitoring, which are based on the recommendations of the penetration testers.[6] The main issue is the ignorance of the essential principles of cybersecurity in connection with the wrong understanding of the protection against cyber attacks in the area of the intelligent public transport service, which can be demonstrated on the outcomes of the European Union Network and Information Security Agency (ENISA) study on Cybersecurity and Resilience of Intelligent Public Transport. The study outcomes results in surprising finding, that 40 % of respondents confirmed hypothesis, that company at which they work does not test the functionality of the measures in the cybersecurity area.[7]

As the primary research question, which will be examined in this article, is to identify the risks associated with cyber attacks in international transport. A secondary research question will be to determine whether and to what extent the consequences of cyber attacks in international transport can be reduced using insurance.[8]

The research in this article will be based on research of the literature, when an analysis of the sources of the legislation, professional literature and Internet resources will be provided. The sources of information used will be subjected to critical evaluation and, based on a synthesis of the acquired knowledge, the author's own opinions will be expressed.

The primary research question will be solved in the theoretical part of this article on the basis of definition and analysis of cyber risks threatening in different modes of transport (case study approach). The secondary research question will be answered with the use of the comparative analysis. The author will look for answer to question, if the recent state of the cyber security risk in international transport could be reduced by the cyber risk insurance. As part of the assessment of the possibility of mitigating the risks associated with cyber attacks

[5] The security challenges in this area are in more detail analysed in Harvey, J., Kumar, S. (2020) A Survey of Intelligent Transportation Systems Security: Challenges and Solutions, Conference paper, May 2020, [online]. Available from: https://www.researchgate.net/publication/342405096 [Accessed 10 November 2021].

[6] Cf. U. S. Department of Transportation. (2019) Cybersecurity and Intelligent Transportation System, Best Practice Guide – September 17, 2019, Publication Number: FHWA-JPO-19-763, p. 35 [online]. Available from: www.its.dot.gov/index.htm [Accessed 10 November 2021].

[7] Lévy-Bencheton, C., Darra, E. (2015) *Cybersecurity and Resilience of Intelligent Public Transport, Good practices and recommendations*, Athens: ENISA, pp. 31 and 32.

[8] According to the recent survey 2,78% cyber insurance claims between 2013 and 2019 were located in transportation. (Source: Statista (2021) *Distribution of the number of cyber insurance claims made worldwide between 2013 and 2019, by industry*. New York: Statista Inc. Available from: www.statista.com/statistics/1190969/cyber-insurance-number-claims-industry-global [Accessed 25 June 2021]).

a comparison of insurance coverage offered in the insurance conditions of selected insurance companies will be conducted. To address the aim of this research, in the practical part of this article will be conducted analysis of insurance coverage, risk and premium based on the insurance terms and conditions.

2. THEORETICAL PART – DEFINITION OF CYBER RISKS IN INDIVIDUAL TYPES OF TRANSPORT

2.1 AIR TRANSPORT

2.1.1 INTRODUCTION TO CYBER RISKS IN AIR TRANSPORT

According to the press report published in 2015 was possible to successfully hack the guidance system of civil aeroplane due to lack of security software via universal series bus port mounted on the back of the passenger seat. The affected aeroplane control systems allowed the perpetrator experimentally change the trajectory of the flight. [9]

2.1.2 INTERNATIONAL REGULATION OF THE PROTECTION OF AIRCRAFT FROM CYBER ATTACKS

International governmental organisations are looking for solution based on the education and skill oriented training. The International Air Transport Association (IATA) clearly stated that increased reliance on data and connectivity will further exacerbate cyber security risks.[10] On that ground IATA created set of guidelines to mitigate cybersecurity risks[11]. It is a overview of international cyber security instruments, documents, standards and guidelines applicable to Civil Aviation Sector with recommendations and short commentaries. The cybersecurity in international air transport is also the strategic objective of the International Civil Aviation Organisation (ICAO). The ICAO introduced its Aviation Cybersecurity Strategy in October 2019.[12] The Aviation Cybersecurity strategy is based on seven pillars (1. International cooperation, 2. Governance, 3. Effective legislation and regulations, 4. Cybersecurity policy, 5. Information Sharing, 6. Incident

[9] Weise, E. (2015) Officials look into whether hacker really took over plane. *USA Today*, 17 May. Available from: https://eu.usatoday.com/story/tech/2015/05/17/hacker-sideways-chris-roberts-fbi-united/27492409/ [Accessed 21 June 2021].

[10] IATA, Airport Transport Security 2040 and Beyond, Version 1, 2019, p. 9.

[11] IATA. Compilation of Cybersecurity Regulations, Standards, and Guidance Applicable to Civil Aviation, Edition 2.0, April 2021.

[12] ICAO, Aviation Cybersecurity Strategy, Quebec, October 2019, p. 2-4.

management and emergency planning, 7. Capacity building, training and cybersecurity culture). ICAO also earlier issued working papers containing, in an annex, the Assembly's resolution on cybersecurity in civil aviation[13]. The problem is that the Action Plan on Cybersecurity in Civil Aviation only broadly declares a commitment to cooperation between the contracting states, which is specified in the Appendix A (Cybersecurity Action Plan Roadmap). ICAO should develop cybersecurity policy guidance to facilitate harmonisation and consistency amongst global, regional and national policies. National specific aspects ought to be justified and facilitate transnational compliance (Art. 7.3.1.). ICAO will conduct a review of the Action Plan on Cybersecurity in Civil Aviation as and when appropriate, but the Member States of ICAO cannot be sanctioned for noncompliance with the measures stipulated in the Action Plan. ICAO relies on content of arguments during intensive communication with the Member States,[14] allowing enforcement of measures scheduled in Appendix A. The priority should be given to work towards a common baseline for cybersecurity standards. According to the Art. 37 of the Convention on International Civil Aviation "*International Civil Aviation Organization shall adopt and amend from time to time, as may be necessary international standards and recommended practices*" dealing with i.e. communications systems and air navigation aids, rules of the air and traffic control practices, and such other matters concerned with the safety, regularity and efficiency of air navigation.

The Assembly's resolution on cybersecurity in civil aviation was adopted by the ICAO General Assembly at its meeting in the period from 27 September 2016 to 6 October 2016 in Montreal under No. A39-19. The Assembly's resolution on cybersecurity is also only of a recommendatory nature and, in addition, the activities set out therein were implemented by the 40th session of the ICAO General Assembly (Resolution A40-10: Addressing Cybersecurity in Civil Aviation), which took place from 24 September 2019 to 4 October 2019 and resulted in the approval of the ICAO Cybersecurity Strategy, which is again

[13] ICAO Working paper, Assembly – 39 Session, Executive Committee, Agenda Item 16: Aviation Security – Policy, Addressing Cybersecurity in Civil Aviation, A39-WP/17 EX/5, 30. 5. 2016, which was subsequently amended in the form of the ICAO Working paper, Assembly – 40 Session, Executive Committee, Agenda Item 12: Aviation Security – Policy, ICAO Cybersecurity strategy, A40-WP/28 EX/13, 25. 6. 2019.

[14] ICAO has 191 Member States recently.

of a recommendatory nature in relation to the Member States. In particular, ICAO calls on States Parties and civil aviation entrepreneurs to participate in the development of strategies to combat cyber crime, the establishment of governmental and non-governmental bodies to share information and minimise cyber risks, and the drafting of international and national legislation to protect against cyber risks in international aviation transportation.

The Study Group on Cyber Security in Civil Aviation (CYBER) is trying since 2013 to raise the level of awareness of cyber risks in European Civil Aviation Conference (ECAC) Member states.[15] On that ground the Study group is analysing recent developments of cyber-security control measures and giving guidance how to reduce risk of cyber-security attacks aimed on the critical aviation information systems.

2.2 MARITIME AND RIVER TRANSPORT

2.2.1 INTRODUCTION TO MARITIME CARGO TRANSPORT

In 2019, 7,907,300,000 tonnes of dry goods, 1,860,200,000 tonnes of crude oil, and 1,308,400,000 tonnes of refined petroleum products, gas and chemicals was transported by sea[16]. It is therefore surprising how inadequate the security measures on board cargo ships and in ports are. The state bodies[17] and bodies of governmental and non-governmental international organisations are implementing measures in order to the cyber risks[18].

2.2.2 ELECTRONIC SYSTEMS USED FOR THE CONTROL, COMMUNICATION AND NAVIGATION OF MARITIME AND RIVER VESSELS

System for displaying electronic navigational charts and information

The Electronic Chart and Display Information System[19] (ECDIS) is an electronic assistance system employed in the management of vessel. The cybersecurity of the ECDIS system is often underestimated by the ship--owners, who are implementing software and hardware components

[15] ECAC Doc. 30, chapter 14.

[16] Source: Barki, D. and Deleze-Black, L. (ed.) (2020) Developments in International Seaborn Trade. *UNCTAD Review of Maritime Transport 2020*, p. 7.

[17] E.g. in the United States of America this refers to the U. S. Department of Homeland Security.

[18] An example may be the IMO Guidelines on Maritime Cyber Risk management (IMO's Maritime Safety Committee, MSC-FAL.1/Circular 3, 5. 7. 2017), or the BIMCO Guidelines on Cybersecurity Onboard Ships (version 4, 2020).

[19] Note: The ČSN EN 61174 ed. 3 (367827) standard uses the translation System of Electronic Chart and Information Display.

of the navigational devices.[20] The ECDIS software is representing a security risk to ship navigation technology systems, which can be easy target for the cyber attack, because this software is simply integrated to the operational system of the on-board computer. ECDIS constitutes critical operational technology (software) designed for planning of the maritime voyage.[21] Crew management and members need to get basic safety training in order to prevent breach of discipline during the long voyages. Some crew members of maritime ships use USB ports connected to the ECDIS to play on-line computer games and to communicate with their families via smart phones, which may lead to interruption or collapse of the whole navigational system as a result of such activity[22].

Automatic identification system

In the maritime sector is used since 2002 as the supplement of the navigation systems the Automatic Identification System (AIS) which allows real-time location tracking of the vessels. The system provides important information related to the position of the ships for shore-based broadcasting stations and coastal authorities which is crucial for safe operation and anchoring of ships in their vicinity. The vessels equipped with AIS have possibility to locate the position of the ships within the distance of 20 nautical miles, even if they cannot be seen by the radar. The advantage and disadvantage of the AIS is, that the information's about the ship (course, position registration number etc.) could be found easily via many internet webpages, which are accessible without password and free of charge. The security risk rests in the AIS messaging system, which is unencrypted. It means, that messages including sensitive information, can be obtained by the hijackers (or pirates) with relatively cheap high frequency receiver.[23]

Global navigation system

---

[20] Svilicic, B., Brčić, D., Žuškin, S, Kalebić, D. (2019) Raising Awareness on Cyber Security of ECDIS, *TransNav*, 13 (1), p. 231.

[21] DiRenzo, J. et al. (2015) The *Little-known Challenge of Maritime Cybersecurity*. [online], p. 2. Available from: http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyber CorfuPaper.final.pdf [Accessed 4 January 2021].

[22] *The Nautical Institute*. Charging your phone on the bridge? Think again!, The Navigator, June 2016, pp. 6-8.

[23] Kessler, G. C., Craiger, J. P., Haas, J. C. (2018) Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System, *TransNav*, 12 (3), p. 432.

The Global Positioning System (GPS) is used as part of the AIS, that is why both systems can be affected by the same cyberattack. The dangerous hacker activities are focused merely on spoofing of the GPS system, because the jamming of this system leads to activation of the automatic alert system within the vessel's GPS module. The spoofing of the GPS may result in a fatal accident, which can be demonstrated on the maritime incident reported in the Black Sea in 2017.[24] For a few days GPS navigation devices gave an inaccurate inland position near Gelendyhik airport instead of correct position 25 nautical miles far away from it. In this context, should be mentioned experiment within the University of Texas project[25], as part of which a deliberately fraudulent signal was sent to a luxury yacht called "White Rose of Drax", whose automatic control system changed the course of the vessel in the wrong direction upon receipt[26]. For the disruption of the GPS signal is no need of very advanced capabilities, because the signal is usually very weak.[27] Hackers may also completely block the reception of signals by ships with outdated hardware and software.[28]

2.2.3 INTERNATIONAL REGULATION OF THE PROTECTION OF MARITIME VESSELS FROM CYBER ATTACKS

The International Ship and Port Facility Security Code was adopted on 12 December 2002 during the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea (1974). The main objective of the code is to establish an international framework for detection and assessment of security threats including preventive measures against security incidents affecting ships or port facilities. International Maritime Organization (IMO) amended the International Ship and Port Facility Security Code[29] and the International Safety Management Code[30] in reaction

[24] Goward, D. (2017) Mass GPS Spoofing Attack in Black Sea? [online]. Available from: www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea [Accessed 26 November 2021].

[25] Press release on the project was published on 29. 7. 2013 at: www.news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/ [Accessed 4 January 2021].

[26] Muccin, E. (2015) *Combatting Maritime Cybersecurity Threats*. [online]. Available from: http://magazines.marinelink.com/Magazines/MaritimeReporter [Accessed 4 January 2021].

[27] Hambling, D. (2017) Ships fooled GPS spoofing attack suggests Russian cyberweapon *New Scientist* [online]. Available from: www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/ [Accessed 4 November 2021].

[28] Dobiáš, P. (2019) Kybernetická bezpečnost v mezinárodní přepravě se stále podceňuje, *Logistika*, 25 (1), p. 27.

[29] Revised version of 2017.

[30] International Safety Management Code, edition 2018, ID117E.

to increased incidence of cyberattacks. Here should be mentioned three fundamental problems specified by V. L. Forbes, which are related to the security of maritime vessels against cyberattacks. These include the obsolescence of maritime vessels' operating systems, the lack of training for vessel operating staff pertaining to management and protection against cyber attacks, and the lack of security for land-based communication facilities for maritime vessels[31]. Rolls Royce intends to gradually put into operation from 2021 remotely controlled autonomous vessels onwards, in order to reduce risk of a loss caused by the human element to a minimum. Information on the security of these vessels against cyber attacks is logically not known with regard to the company safety policy.[32]

2.3 ROAD TRANSPORT

2.3.1 INTRODUCTION TO CYBER RISKS IN ROAD TRANSPORT

The modern autonomous vehicles use specific deep reinforcement learning techniques for better recognition and avoidance of collision with obstacles, which could be remotely controlled by the perpetrator.[33] Recently were reported new security flaws in versions of Ford Focus and Volkswagen Polo, which can lead to data loss and malfunction of the electronic car management system. As the most vulnerable part of the car was proven the infotainment vehicle's system, which allows direct access to the personal data of the car owner and disabling of the automatic traction system.[34] This case demonstrates that drivers and passengers can be endangered by an attack on the system used to provide traffic and entertainment information to the driver and service information to the vehicle manufacturer.

An attack on a truck or a bus can also pose a really serious risk, given that efforts are being made to autonomously drive and automatically park

---

[31] Forbes, V., L. (2018) The *Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges*. [online] Available from: www.futuredirections.org.au/publication/the-global-maritime-industry-remains-unprepared-for-future-cybersecurity-challenges/ [Accessed 4 January 2021).

[32] Walker, J. (2018) *Autonomous Ships Timeline – Comparing Rolls-Royce, Kongsberg, Yara and More*. [online]. Available from: www.techemergence.com/autonomous-ships-timeline [Accessed 4 January 2021].

[33] Hahn, D., A., Munir, A., Behzadan, V. (2021) Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges, *IEEE Intell. Transp. Syst. Mag.*, 13 (1), p. 7.

[34] Which. (2021) Popular connected cars from Ford and Volkswagen could put your security privacy and safety at risk, Which? Finds, Which [online]. Available from: https://press.which.co.uk/whichpressreleases/popular-connected-cars-from-ford-and-volkswagen-could-put-your-security-privacy-and-safety-at-risk-which-finds/ [Accessed 26 November 2021].

even these vehicles. To this end, Jeremy Daily[35] recommends the use of a special test environment designed to improve safety standards and identify vulnerabilities in truck electronic control systems.

In road transport, a truck can also be monitored by camera systems located on motorway routes and other major urban and extra-urban roads. Toll and transit systems now automatically recognise and store vehicle registration plates. With the help of these systems, an attacker can not only determine the location of a vehicle, but also its speed, because many road camera systems are connected to devices for measuring the maximum permitted speed. This allows criminals to monitor a vehicle and more easily plan the act of physically breaking into a vehicle or a suitable moment to attack its control systems. Given that, in accordance with Article 7 of Regulation No. 561/2006[36], a truck driver must take a safety break after 4.5 hours of driving, perpetrators of criminal activity can calculate the time and place of that break relatively accurately. In addition, they can monitor the vehicle repeatedly and see if the driver leaves the vehicle in an unsecured place at night during transit. If the human driver is replaced by fully autonomous trucks, there is a danger not only of the possibility of remote control of the vehicle control unit[37], but also of the possibility of physically placing the perpetrator's device on the vehicle, if the perpetrator switches on the red light of traffic lights that the autonomous vehicle will pass through. A countermeasure may be to place a sufficient number of cameras and sensors on the truck. However, if the perpetrator manages to penetrate the vehicle's control system, he will usually control or paralyse these systems as well.

2.3.2 INTERNATIONAL REGULATION OF THE PROTECTION OF ROAD TRANSPORT FROM CYBER ATTACKS

On 22 January 2021 entered into force three UN vehicle regulations adopted by the World Forum for Harmonization of Vehicle Regulations created

[35] Daily, J. et al. (2016) Towards a Cyber Assurance Testbed for Heavy Vehicle Electronic Controls. *SAE International Journal of Commercial Vehicles*, 9 (2), p. 58.

[36] Regulation (EC) No. 561/2006 of the European Parliament and of the Council of 15 March 2006 on the harmonisation of certain social legislation relating to road transport and amending Council Regulations (EEC) No. 3821/98 and (EC) No 2135/98 and repealing Council Regulation (EEC) No 3820/85 *Official Journal of the European Union* (2006/L-102/1).

[37] The fact that even a sophisticated autonomous control system can be deceived was demonstrated in the past on a Tesla vehicle (Greenberg, A. (2016) *Hackers Fool Tesla S'S Autopilot to Hide and Spoof Obstacles* [online] New York: Wired. Available from: www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles [Accessed 4 January 2021].).

within the framework of United Nations Economic Commission for Europe (UN Regulation No. 155 concerning the approval of vehicles with regards to cyber security and cybersecurity management system, UN Regulation No. 156 Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system and UN Regulation No. 157 on the type approval of automated lane keeping systems). This important legislative activity, which is based on the system of minimum requirements laid out especially in the above mentioned regulations No. 155 and 156, is limited to the Member states of UNECE only. But there it is assumed,[38] that regulators in Non-member states will be influenced by the UNECE standard.

The Regulation No. 156 covers all crucial aspects of cybersecurity across the entire motor vehicle lifecycle (management of cyber risks, ensuring security of vehicles by design, detection and response to security incidents and ensuring of safe software updates).

2.4 RAIL TRANSPORT

2.4.1 INTRODUCTION TO CYBER RISKS IN RAIL TRANSPORT

The Annex (Chapter V. Section B.) to the Regulation No. 432/2010 Coll., on the Criteria for Determining Critical Infrastructure Elements classify the Railway infrastructure as the element of critical transport infrastructure[39] (the critical infrastructure is defined in the Czech Republic in Act No. 240/2000 Coll., the Crisis Act, as the element of the critical infrastructure, or a system of critical infrastructure elements. The disruption

[38] Cf. Burkacky, O., Deichmann, J., Klein, B., Pototzky, K., Scherf, G. (2020) Cybersecurity in automotive: Mastering the challenge, report, McKinsey&Company, p. 7. Available from: www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge# [Accessed 24 June 2021].

[39] According to the Annex II of the Directive (EU) of the European Parliament and of the Council of July 2016 concerning measures for high common level of security of network and information systems across the Union (NIS Directive) railway undertakings and infrastructure managers are classified as operators of essential services within the meaning of Art. 4 (4), if they meet the criteria laid down in Art. 5 (2). The criteria for the identification of the operators of essential services shall be: an entity provides a service, which is essential for the maintenance of critical or/and economic activities; the provision of that service depends on network and information systems; and an incident would have significant disruptive effects on the provision of that service. The Member States shall adopt and publish by 9 may 2018, the laws, regulations and administrative provisions necessary to comply with NIS Directive. E.g. in Germany is recognised railway infrastructure also as very important part of critical infrastructure (Regulation of 22 April 2016 for determination of Critical Infrastructure according to the BSI-Act. Federal Ministry of the Interior, Building and Community and Federal Ministry for Economic Affairs and Energy. In German.). This Regulation contains specific parameters for evaluation of the railway sites as the elements of critical infrastructure based on the number of passengers or weight of transported goods.

of the critical infrastructure could have a serious impact on the security of state, the provision of the basic living needs of the population, human health or state economy. This part of critical infrastructure needs special protection against cyber attacks, because of its vulnerability.[40] Today the technical state and position of the train is controlled by the track and rail monitoring systems and suitable measures can be initiated even before rail operations are negatively impacted. Functions such as real-time monitoring and tracking of railway vehicles can improve the overall rail system reliability,[41] but the railway management and control systems can be also hacked by criminals, who are motivated by a bid to obtain funds,[42] The cyberwarfare driven by political motivations could be found also in the railway sector.[43] We can speak about increasing threat of the terroristic attacks against high speed trains.[44]

2.4.2 INTERNATIONAL REGULATION OF THE PROTECTION OF RAILWAYS FROM CYBER ATTACKS

Within the COLPOFER[45] were created different working groups for the purpose of detection, prevention and elimination of security vulnerabilities in railway sector (e.g. cybercrime, terrorist and extremist activities). The main tasks of the working group established for prevention of cybercrime is to facilitate exchange of knowledge and information related to cybercrime in railway sector and to create recommendations regarding

---

[40] Fuchs, P. Rozová, D., Šustr, M., Šohajek, P. (2018) Critical Infrastructure in the Railway Transport System, Proceedings of the 22nd World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2018), p. 184.

[41] Ulianov, C., Hyde, P., Shaltout, R. E. (2018) Railway Applications for Monitoring and Tracking Systems. In: Marin Marinov (ed.) *Sustainable Rail Transport, Lecture Notes in Mobility*, Cham: Springer International Publishing, 2018, pp. 77-91.

[42] This conclusion could be demonstrated on recent cases in Czech Republic (David, J. (2021) Cyber Attack on Railways in the Czech Republic. Railtarget, 22 March [online] Available from: https://www.railtarget.eu/news/cyber-attack-on-railways-in-the-czech-republic-215. html [Accessed 24 June 2021]) and in United States of America (Goldbaum, Ch., Rashbaum, W. K. (2021) The M.T.A. Is Breached by Hackers as Cyberattacks Surge. New York Times, 2 June [online]. Available from: https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html [Accessed 24 June 2021]).

[43] Clear example are Madrid train bombings (first attack was carried out on 11th March 2004). The second bombing on 2nd April 2004 directed against high-speed AVE train was not successful.

[44] In the United States was published already in 2006 study on Freight and Passenger Rail Critical Infrastructure Assessment warning over underfunding for security enhancements of all systems in American Public Transportation (Capra, G. S.: Protecting Critical Rail Infrastructure. The *Counterproliferation Papers*, Future Warfare Series No. 38, USAF Counterproliferation Center, p. 11), which exemplifies the initial underestimation of preventive measures in highly developed economy.

[45] This organisation operates in Europe and is one of the specialised groups within the International Union of Railways (UIC).

data protection. The European Union supported the Cybersecurity in the Railway Sector Project (CYRAIL), which was finished in 2018. During the international conference held in Paris (UIC Headquarters, 18 September 2018) were presented CYRail Recommendations on the cybersecurity of signalling and communication systems.[46] The main benefit to railway security is the CYRail Recommended system. The recommended security model is designed as alerting and collaborative 3-tier management system (1. detection system, 2. centralized alerting and monitoring system and 3. collaborative information sharing system).

2.5 PARTIAL CONCLUSION

Based on the analysis carried out during the preparation of this article, it was found that international transport faces insufficient training of staff operating means of transport[47] and the insufficient or even complete lack of security against cyber attacks. How else can it be explained that some vehicle crews use USB ports designed to update control system software to communicate on social networks[48] via their own devices?

There is still the idea, even among a large number of entrepreneurs, especially in maritime and air transport, that a means of transport far away from transmitters cannot be the target of a cyber attack. The cost incurred to protect against cyber attacks is low compared to the damage that a hacker attack can do. Obsolete means of transport can be easily exposed to cyber attacks if at least regular security software updates are not performed[49].

---

[46] CYRail Consortium Members. CYRail Recommendations on cybersecurity of rail signalling a communication systems. UIC-ETF, September 2018, ISBN 978-2-7461-2747-0.

[47] In the recent study on cyber security in transport by rail prepared within the EPSF (Établissement public de secúrité ferroviaire) was confirmed, that access required by maintenance staff must be brought under control (Établissement public de sécurité ferroviaire (2021) *Taking cybersecurity challenges into account in railway safety*. ENR135 – V1. Amiens: European Union Agency for Railways (ERA), French National Cybersecurity Agency (ANSSI), French National Safety Agency for Railways (EPSF), and SNCF Voyageurs and SNCF Réseau, p. 16).

[48] *The Nautical Institute*. Charging your phone on the bridge? Think again!, The Navigator, June 2016, pp. 6-8. Press release on the project was published on 29. 7. 2013 at: www.news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/ [Accessed 4 January 2021].

[49] For the sake of completeness, it is necessary to state that some transport companies cannot update the operating system without testing a new update of the operating system, because otherwise the operating system may crash (On this issue, compare Šulc, V. (2018) *Kybernetická bezpečnost*. Pilsen: Aleš Čeněk, pp. 95 and 96). This does not change the fact that most of the vulnerabilities that are subject to a cyber attack have been known for a long time at the time of the attack and are therefore not so-called day zero vulnerabilities.

Nor is it gratifying to note that sufficient importance is not placed on protection against cyber attacks at the international level, because significant expenses required for sufficient protection against cyberattacks, will raise the transport costs. In view of the costs required for hardware and software security, documents of a recommendatory nature are being developed within working groups and left to national legislation[50] as to how to regulate protection against cyber risks. Despite the European Union's efforts to regulate this area by secondary law and by supporting projects aimed at cybersecurity, the state of protection against cyber attacks is still insufficient.

3. PRACTICAL PART – MITIGATION AND ELIMINATION OF RISKS IN INTERNATIONAL TRANSPORT THROUGH INSURANCE

3.1. DEFINITION OF CYBER RISKS IN INTERNATIONAL TRANSPORT

In international civil transport may be subject to a cyber attack telematics – especially audio and visual equipment (traffic lights, audio warning equipment, traffic signals with variable display, etc.) and some other traffic equipment (barriers, inlet closures, locks, automatic sliding bollards, lifting bridges, etc.). Usual subject of a cyber attack are also means of transport in road, air, rail, maritime and inland waterway transport. Within the maintenance and operation of vehicles is required protection of service stations and filling stations for the pumping of fossil fuels or the charging of electric vehicles. Specific measures shall be adopted for protection of public transport stations and computer systems used to record passengers, baggage and goods. The necessity for strict measures could be demonstrated on Air India,[51] Brittish Airways[52] and Lufthansa[53] personal data leaks. The attention shall be paid to protection of infrastructure

[50] According to § 2(i) of Act No. 181/2014 Coll., on cybersecurity, a basic service is a service the provision of which depends on electronic communication networks or information systems, and whose disruption could have a significant impact on the security of social and economic activities, e.g. in the transport sector.

[51] Page, C. (2021) Air India Data Breach: Hackers Access Personal Details Of 4.5 Million Customers. *Forbes*, 23 May. Available from: https://www.forbes.com/sites/carlypage/2021/05/23/air-india-data-breach-hackers-access-personal-details-of-45-million-customers/ [Accessed 25 June 2021].

[52] MacGregor, L. (2019) British Airways faces largest ever data breach fine for 2018 hack. *New Scientist and Press Association.* 8 July. Available from: https://www.newscientist.com/article/2208964-british-airways-faces-largest-ever-data-breach-fine-for-2018-hack/ [Accessed 25 June 2021].

necessary for proper and safe functioning of all modes of transport (warehouses and transhipment points, including their equipment – e.g. cranes and trucks, traffic control centres – airport navigation towers, radars, sea beacons and stationary or portable navigation systems).

The cyber attacks can disable security devices used to detect the danger of fire, accidents of means of transport, etc., which are crucial for mitigation of damages and personal injury.

In the case of a cyber attack on the equipment listed in previous paragraph, the following consequences may occur, for example:

a) traffic accidents at an intersection or railway crossing due to non--functioning signalling and security,
b) control of the vehicle by the attacker and its destruction, damage or theft,
c) explosion of a filling station, leakage of dangerous substances, or refueling of fuel or energy by a perpetrator free of charge,
d) inoperative service mechanism preventing the repair of vehicles or causing damage to them,
e) theft of goods from a warehouse or control of their equipment and causing of damage,
f) stopping public transport of persons, or guiding means of transport into a collision course resulting in an accident, or controlling air conditioning or a fire extinguishing system,
g) causing a navigation system to malfunction, resulting in the need to switch to manual backup systems and controls with an increased risk of accidents,
h) transmission of a false GPS signal in order to change the course of the autopilot,
i) misuse of passenger information (personal data, data from a means of payment, etc.) for the purpose of the use of such data, sale or extortion,[54]

[53] DPA/AFP. (2015) Hackers break into Lufthansa customer database. *Deutsche Welle*,10 April. Available from https://www.dw.com/en/hackers-break-into-lufthansa-customer-database/a-18374698 [Accessed 25 June 2021].

[54] S. Wares and V. Thompson, are mentioning loss and deletion of data, which could be consequence of non-payment for unblocking of encrypted passengers database (Wares, S., Thompson, V. (2015) *Marsh Insights: Cyber Risk in the Transportation Industry*, p. 1 [online]. Available from: https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20.Transportation%20Industry-03-2015.pdf [Accessed 4 January 2021]).

j) dysfunction of the security equipment enabling the prevention of collisions of vehicles or their fire.

Gina Tonn, Jay P. Kesan, Jeff Czajkowski and Linfeng Zhang[55] present the following general ways to prevent cyber damage:

a) development of methods that will improve the system architecture and activities,
b) operating methods involving changes in business transactions,
c) countermeasures, including the acquisition of security software, the design of the system, the improvement of the course of operations and investment in the cybersecurity workforce,
d) security measures including firewalls, encryption software, a virus detection system, and the division of the system into several parts.

As another possible breakdown of cyber risk management measures, they[56] state the division into:

a) institutional measures (software and hardware),
b) procedural measures (management systems and operating systems),
c) responsive measures (response and damage management after a security incident has been detected).

The above authors come to the unequivocal conclusion that the growing number of cyber attacks and the damage they cause will lead to efforts to transfer risk to insurance companies through cybersecurity insurance, especially for entrepreneurs[57,58]. What cannot be fully agreed with is the claim of these authors that a risk is arising that policyholders will not take sufficient measures in the field of cybersecurity, as they will rely on insurance companies to compensate for the damage they cause.[59] Given that insurance companies are likely to want part of the insurance portfolio

[55] Tonn, G., Kesan, J. P., Czajkowski, J. and Zhang, L. (2018) *Cyber Risk and Insurance for Transportation Infrastructure*, p. 3 [online]. Available from: https://riskcenter.wharton.upenn.edu/wp-content/uploads/2018/03/WP201802_Cyber-Security-Transportation-Sector.pdf [Accessed 4 January 2021].

[56] Ibid, p. 4.

[57] Ibid, p. 3.

[58] We can find contrary opinion in the study of K. Quigley and J. Roy, who are disputing possibility to use insurance for the transfer of risk to insurance company, because „the failures are too difficult to model, and therefore impossible to cost" (Quingley, K., Roy, J. (2011) Cyber-Security and Risk Management in an Interoperable World An Examination of Governmental Action in North America, *Social Science Computer Review*. 30 (1), p. 86. Available from: http://ssc.sagepub.com/content/30/1/83 [Accessed 24 June 2021]).

[59] Transfer of risk is recognised as one of five main risks control strategies (Cf. Kure, H. I., Islam, S., Razzaque, M. A. (2018) An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*, 8 (6), p. 16. Available from: www.mdpi.com/2076-3417/8/6/898 [Accessed 25 June 2021]).

comprised by insured cyber risks to be covered by reinsurance, it can be expected that, given the principle of capital adequacy, reinsurance undertakings will not be willing to take out insurance against insurance of risks for which it is difficult to determine at least the approximate scope of the damage. Insurance companies will therefore require, particularly for insurance of large insurance risks within the EU, that insurers take measures to reduce the probability of the occurrence of an insured event. Large insurance risks are defined in the Solvency II Directive[60] as a group of risks which are typically arising out of entrepreneurial activities. According to Article 13 (27) of the Solvency II Directive, large insurance risks include, inter alia, insurance of railway rolling stock, aircraft and vessels, including the goods transported and liability for the use of such means of transport[61]. However, it is difficult to determine the extent of damage incurred in transport during previous years. Although data on the number of cyber incidents is available on the Internet[62], only few statistics specify the resulting damage.[63,64] The uncertainty posed by the abovementioned issues arising out during the process of assessing the insurance risk leads to the situation, that there are few entities that specialise in cyber risk insurance in international transport[65]. In addition, many carriers rely on the fact that unless cyber risk insurance is excluded

[60] Directive (EC) 2009/138 of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) *Official Journal of the European Union* (2009/L-335/01).

[61] Insurance of ground vehicles (besides the railway fleet) is one of the major insurance risks only if the policyholder exceeds the limits for at least two of the criteria set out in Article 13(27) of the Solvency II directive.

[62] According List of data breaches and cyber attacks of 2020 there were reported 15 data breaches in transport and automotive (Irwin, L. (2021) 2020 cyber security statistics, IT Governance Available from: www.itgovernance.co.uk/blog/2020-cyber-security-statistics [Accessed 24 June 2021]).

[63] According to the summarized Assessment report of AIG designed for the client with annual revenue 51.000.000 USD the Data Breach Impact (median impact value per record volume) will be in case of low impact breach 85,712,026 USD for company with 100 millions records (AIG. (2020) *Cyber Insurance Summarized Assessment Report*, American International Group, Inc. Available from: www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-summarized-assessment-report-sample.pdf [Accessed 24 June 2021]).

[64] M. Bentley et al. hold an opinion that only limited data on cyber incidents are available and thus it is very difficult to get data pertaining to the losses suffered by one organization (Bentley, M., Stephenson, A., Toscas, P., Zhu, Z. (2020) A Multivariate Model to Quantify and Mitigate Cybersecurity Risk, *Risks*, 8 (61), p. 2. Available from https://doi.org/10.3390/risks8020061 [Accessed 24 June 2021]).

[65] An example of such a company is Marsh Ltd., an insurance intermediary based in London, which also deals with the assessment of insurance risks in international transport, or Jardine Lloyd Thompson Group plc, also based in London.

under an explicit exemption from insurance coverage, the insurance also covers these insurance risks.[66]

3.2. INSURANCE AGAINST CYBER RISKS IN INTERNATIONAL TRANSPORT

3.2.1. SYSTEMATIC INCLUSION OF CYBER RISK INSURANCE IN INTERNATIONAL TRANSPORT

Cyber risk insurance is non-life insurance[67] from the public law perspective and indemnity insurance from the private law perspective. According to Art. 1:201 (3) of the PEICL,[68] "indemnity insurance means insurance under which the insurer is obliged to indemnify against loss suffered on the occurrence of an insured event." The consequences of the insured event must be measurable in money. The purpose of indemnity insurance is therefore to compensate for loss resulting from an insured event[69]. Within the scope of indemnity insurance for cyber risks it is possible to arrange:

a) property insurance,

b) legal expenses insurance; and

c) liability insurance.

Property insurance will mainly cover means of transport and equipment. Legal expenses insurance will cover the elimination and minimisation of the consequences caused by a cyber attack, e.g. in the event of data leaks from a database of clients[70] and passengers, or in the case of legal representation costs in damages proceedings against a hacker. Liability

---

[66] In the study on silent cyber coverage in insurance provided by Leibnitz University Hannover - Institute for Risk and Insurance (Wrede, D., Stege, T., Graf von der Schulenburg, J.-M. (2020) Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. The *Geneva papers on Risk and Insurance – Issues and Practice*, 45 (4), p. 657-689. Available from: www.repo.uni-hannover.de/handle/123456789/10772 [Accessed 24 June 2021]) was confirmed, that German insurers „have not yet developer holistic strategies for managing silent cyber exposures. Silent cyber exposures require systematic identification and quantification since the involved claims burdens are hard to estimate for insurers." This study supports the conclusion, that the cyber insurance is still unexplored branch of insurance designed for specialised insurers.

[67] The same is valid for the classification of risks according to classes of insurance in the framework of Directive Solvency II (Annex I).

[68] Basedow, J., Birds, J., Clarke, M. Cousy, H., Heiss, H. Loacker, L. (2016) *Principles of the European Insurance Contract Law*, 2nd ed., Cologne: Otto Schmidt, pp. 33 and 77.

[69] Karfíková, M. et al. (2018) *Insurance Law*. Prague: Leges, p. 307.

[70] An example is the case of the shipping company OutWest Express, whose computer servers were attacked by ransomware, which allowed hackers to gain access to data from a customer database and to order fictitious transport of goods in order to solicit cash advances from transport agents (Kilcarr, S. (2015) *Battling a hack: One fleet's story*. [online] Fort Atkinson: Fleetowner. Available from: https://www.fleetowner.com/technology/article/21692058/battling-a-hack-one-fleets-story [Accessed 4 January 2021]).

insurance will cover the obligation of the policyholder (carrier) to compensate for the damage arising to the damaged party to the extent and in the amount specified by law or contractual agreement.

3.2.2. CONDITIONS OF CYBER RISK INSURANCE

The insurance conditions of cyber risk insurance have a significantly more extensive structure and contain a more detailed regulation of the rights and obligations of the insurer and the policyholder in comparison with the insurance conditions of the insurance of internet risks concluded as part of household insurance. The content of the general insurance conditions is also a casuistic in its character.[71] The content of these conditions can be demonstrated on the insurance product called CYBERPLUS – CYBER RISK INSURANCE[72] and Cyber Enterprise Risk Management[73].

CYBERPLUS insurance forms the basic coverage, which can be variably extended with modules of optional extension coverage. The basic scope of insurance consists of claims for compensation for the damage caused by unauthorised handling of personal data and confidential information to the insured or his subcontractors, claims against the insured due to a breach of network security, costs of regulatory proceedings[74] and costs of professional services (cyber experts and independent consultants in the fields of law, media strategy, crisis management and personal relations).

Insurance coverage can be extended by the following areas:

a) publishing digital content in multimedia,

b) blackmail through a computer network,

c) network failure.

The insurance conditions of Cyber Enterprise Risk Management include the scope of insurance coverage, which in principle corresponds to CYBERPLUS insurance. It is therefore an insurance covering

---

[71] Romanosky et al. in their study focused on insurance policies from state insurance commissioners across New York, Pennsylvania, and California found that the covered losses appeared more consistent across all policies, whereas exclusions were more varied (Romanosky, S., Ablon, L., Kuehn, A., Jones, T. Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity*, 5 (1), p. 4. Available from: https://doi.org/10.1093/cybsec/tyz002 [Accessed 23 June 2021]).

[72] Insurance conditions of Colonnade, version CP 01-05/2019.

[73] Insurance conditions of Chubb European Group, version ERM 1-2016.

[74] According to Article 3.24, regulatory proceedings mean "*any proceedings against the Insured or an investigation or audit of the Insured conducted or carried out by the Supervisory Body (i) due to the use or alleged misuse of Personal Data; or (ii) for the purpose of verifying the procedures for the management and processing of Personal Data; or (iii) arranging such processing via a Subcontractor, to the extent regulated by the Personal Data Protection Guidelines*."

unauthorized handling of data, liability for breaches of network security, media liability, cyber blackmail, loss or corruption of data and interruption of operation.

According to Article 3.11, Cyber Enterprise Risk Management insurance also covers a cyberterrorism attack, while CYBERPLUS does not cover any losses resulting from or otherwise related to war and terrorism according to Article 4.11[75]. In the case of vehicle and equipment insurance, it will also be appropriate to arrange insurance against cyberterrorist attack, because the goal of cyberterrorists may be to take charge of the control systems of an aircraft, train or seagoing vessel in order to obtain a ransom. From the point of view of Czech criminal law, cyberterrorists may commit the crimes of sabotage, a terrorist attack, general endangerment, damage and endangerment of the operation of a public benefit facility or damage to another's property in the transport area[76]. Among the above-mentioned crimes, Václav Jirovský emphasises those that could endanger transport systems, or air traffic, the last of these offenses, as it involves attacks on telecommunications equipment[77]. This view can be accepted, as damage or manipulation to the navigation and communication systems of air traffic control can have fatal consequences, including aircraft crashes.

The limits of indemnity are not specified in the insurance conditions of CYBERPLUS or Cyber Enterprise Risk Management, which can be considered logical with regard to the fact that insurers will arrange this type of insurance according to the individual needs of the policyholder. When arranging special insurance for international transport, the degree of insurance risk is, as a rule, first assessed by means of distance communication. The following is an assessment of the extent of cyber risks related to the person interested in insurance and the determination of proposals for the scope of insurance coverage.

At the same time, the insurer or insurance intermediary simulates, with the person interested in the insurance, situations that may occur in the event of an attack on the means of transport and equipment of the person interested in the insurance. As soon as the person interested in the insurance chooses a suitable variant, a draft agreement containing

[75] As to the definition of the term cyber terrorism, compare Morán Blanco, M., S. (2017) La Ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. *Revista Española de Derecho International*, 69 (2), p. 202.

[76] Smejkal, V. (2018) *Kybernetická kriminalita,* 2nd ed. Pilsen: Aleš Čeněk, p. 104 f.

[77] Jirovský, V. (2007) *Kybernetická kriminalita*. Prague: Grada, p. 95.

a detailed specification of the cyber risks covered by the insurance and exclusion from the insurance, is ready for this potential insured to sign.

3.3. INSURANCE RISK AND PREMIUM AMOUNT

It is difficult to ensure the complete cybersecurity in the case of international transport insurance. There is a need not only for effective software security but also to ensure physical security in the case of this type of insurance, more than in other cases. In the case of securing a means of transport, it will be necessary to effectively prevent the perpetrator from entering, in particular, the vehicle's control systems and the traffic management system. The problem is that a means of transport has to cover long distances and is parked in places with various levels of security during breaks. The question is how service depots for rail vehicles are secured, from which train carriages often leave marked with graffiti. What obstacle for a cyber criminal is posed by a service door locked with a square key and the entrance door to the driver's cab locked with an ordinary cylinder lock? Another example is airport security. Can an airport whose be considered as being sufficiently secure if amateur photographers had roamed on its apron in the past? What can be the consequences of being able to slide under or throw over a counter adjacent to the security checkpoint at an airport a replica of a military grenade? These security incidents will undoubtedly result in insurance companies requiring the performance of penetration tests and to assess, on the basis of these tests, the insurance risk and determine the amount of the premium individually. According the recently published opinion of M. Eling, M. McShane and T. Nguyen during the risk management process, interaction exists between risk mitigation and the purchase of insurance, that is, insurance purchasers typically pay lower premiums by investing more in risk mitigation.[78]

Jan Kolouch[79] presents a range of four basic measures relating to ensuring physical security:

a) securing the perimeter,

b) access control,

c) internal security,

d) protection of computer systems.

---

[78] Eling. M., McShane, M., Nguyen, T. (2021) Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 24, p. 96. Available from: www.onlinelibrary.wiley.com/doi/epdf/10.1111/rmir.12169 [Accessed 25 June 2021].

[79] Kolouch, J., Bašta, P. et al. (2019) *Cybersecurity*. Prague: CZ.NIC, p. 411.

In the case of international transport, the problem is that the perimeter covers not only the whole airport or port but, as demonstrated above, in the past cyber attacks have succeeded in confusing the navigation system of a maritime vessel, and thus this is also probably possible for aircraft. Nevertheless, it will be primarily necessary to protect means of transport and equipment from cyber attack. The problem is how to protect traffic signals, boom gates and other similar equipment, which often operate in semi-automatic or fully automatic mode, from cyber attack. A similar situation arises in the case of lifting bridges and switches, which today are often controlled only remotely, with no human service staff found in their vicinity that could avert danger in the case of a physical attack to the equipment. It is true that this equipment tends to be monitored via camera systems or is connected to a central security desk, but the risk of deception of motion sensors or camera systems cannot be ruled out. The range of service and security units in the event of a cyber incident is also a problem. The subject of the attack may also be the means of transport themselves – it does not have to be exclusively a propulsion unit. It is also conceivable to deactivate an electronic measuring device on a freezer container or a gyroscopic device monitoring the movement of a container with an explosive and volatile substance. In the first case, only the transported food can be destroyed, while in the second case, there can be an explosion and damage to the life, health and property of people.

3.4. INSURANCE COVERAGE IN THE CZECH REPUBLIC AND THE UNITED KINGDOM

Insurers domiciled in the United Kingdom have wide experience with the cyber insurance. For this reason the insurers place emphasis on claim prevention of cyber incidents[80] and mitigation of damages caused by hacker. Efficient standard instrument offered by the insurance companies is 24/7 hours help desk for customers,[81] allowing policyholder to get immediate advice in case of imminent or ongoing attack. Customers

[80] J. Barlatier holds the view, that „*the prevention of cyber threats by private actors is based on risk anticipation and the immediacy of the threats.*" (Barlatier, J. (2020) Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime. *Risks*, 8 (99), p. 8. Available from https://doi.org/10.3390/risks8030099 [Accessed 23 June 2021]) This approach to cyber insurance is evident with regard to many instructional material provided by British insurers free of charge via internet (booklets, manuals, guidelines, statistics etc.).

[81] In the Czech Republic is 24/7 customer support offered in the insurance of cyber risks by ČSOB Pojišťovna (General Insurance Conditions – Insurance of Cyber Risk, version VPP CRC 2018).

who are using help desk can also consult adviser for the purpose of adoption adequate precautionary measures. This access of insurers allows quick response to data or system breach, coverage of the costs associated with fines, ransom payments or notifications, which can be damaging to business of transport company, both in financial and reputational terms. The English insurers are trying by the way of preventive measures to reduce the risk of a loss to a minimum.[82] The insurers are publishing recommendatory publications, which are available free of charge on the internet not only to own customers but also potential customers and general public. The British insurers are providing customers with explanatory booklets in order to prevent misunderstanding and conflicts (e.g. in relation to software updates, firewall protection and virus protection).

Cyber insurance coverage is divided between first-party liability coverage (e. g. business interruption, cyber incident response, digital data recovery, network extortion, telephone toll fraud) and third-party liability coverage (e. g. cyber liability, media liability, network liability, privacy liability, regulatory proceedings).[83] Because of the competition between the insurers domiciled in the United Kingdom, the insurance cover tends to be all-encompassing including first party cover, third party cover, call centre costs, cyber terrorism, increased costs, employee data, reputational harm and transmission of computer virus.[84] The wide insurance cover is often subject to exemptions included in the insurance conditions which

[82] This recent trend was confirmed in report prepared for the Association of British Insurers (Oxera. (2020) The value of cyber insurance to the UK economy, Oxford: Oxera Consulting LLP, p. 12. Available from: www.oxera.com/insights/reports/the-value-of-cyber-insurance-to-the-uk-economy/ [Accessed 23 June 2021]).

[83] Cf. also theoretical concept of differences between first-party liability coverage and third-party liability coverage in Romanosky, S., Ablon, L., Kuehn, A., Jones, T. Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity*, 5 (1), p. 5. Available from: https://doi: 10.1093/cybsec/tyz002 [Accessed 23 June 2021]).

[84] Cf. AIG CyberEdge, version 010719 of 2019; Aviva Insurance Limited, Your insurance policy, version BCOAG 15628 (V36) 02.2021; HISCOX Cyberclear, Cyber and data insurance - policy wording, version WD-PIP-UK-CCLEAR(1) 19029 12/18; Markel UK Limited, Cyber and data risks, version CDR122016; NIG Cyber cover policy, version NIG101423/10/19.

shall be modified[85] according to the specific interest of the policy-holder (cyber policy is sometimes modular).[86]

To compare insurance coverage, we will choose the insurance conditions of Hiscox Limited for cyber and data protection[87]. Although this is an insurance company operating in the United Kingdom, the scope of insurance coverage is, as far as its basic elements is concerned, the same as for insurance companies domiciled in the Czech Republic. Insurance coverage includes interruption of connection, interruption of business activities, damage caused by hackers, cyber extortion, protection of personal data and liability in connection with the media. Similar insurance conditions (Cyber Risk Insurance Policy) are offered in the United Kingdom by Royal & Sun Alliance Insurance plc[88]. This is not a surprising finding, as AIG and Chubb European Group essentially operate worldwide and therefore know the insurance conditions of other insurance companies in the area of cyber risk insurance. The difference between the Czech Republic and some countries lies in the length of cybercrime experience, which can be manifested on clear terminology used in the insurance terms and conditions. Statistics in this area are already available abroad and procedures have been tested on how to proceed in the event of a cyber attack[89].

In the United Kingdom, tailor-made insurance for international transport is also offered. An example of such an insurance product is

---

[85] In a structured dialogue with insurance companies European Insurance and Occupational Pensions Authority (EIOPA) came to conclusion, that „vast majority of the insurers surveyed adopt a focused approach to cyber insurance and tailor products according to the client companies size and needs." (EIOPA. Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies. EIOPA, 2. 8. 2018. Available from: www.eiopa.europa.eu/content/understanding-cyber-insurance-structured-dialogue-insurance-companies_en [Accessed 4 June 2021]).

[86] For analysis of negotiations conducted in order to determine whether to underwrite a cyber risk cf. Nurse, J., R., C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S. (2020) The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes, Conference Paper, p. 3. Available from: https://www.researchgate.net/publication/340849886_The_Data_that_Drives_Cyber_Insurance_A_Study_into_the_Underwriting_and_Claims_Processes/link/5f521074a6fdcc9879ca0a2d/download [Accessed 24 June 2021].

[87] HISCOX Cyberclear, Cyber and data insurance - policy wording, version WD-PIP-UK-CCLEAR(1) 19029 12/18.

[88] Cyber protection - policy wording, version UK 05239 A from19 September 2018.

[89] Cf. Egan, R. et al. (2019) Cyber operational risk scenarios for insurance companies. *British Actuarial Journal*, 24, e6, pp. 1-34. Available from: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/C90FF5F4EC6682A01E91F4E63A05F961/S1357321718000284a.pdf/cyber_operational_risk_scenarios_for_insurance_companies.pdf [Accessed 4 January 2021].

Shoreline Ltd's Integrated Cybercrime Insurance[90] for maritime transport[91]. This insurance covers costs incurred in connection with cyber theft, social engineering, interruption of business activities, investigation, extortion claims, liability for damage caused by third parties, mitigation of the consequences of a cyber attack and costs incurred without delay by the policyholder on minimising damage caused by data leakage, computer system malfunctions and breaches of third party privacy and security. It is interesting to note that the insurance cover applies to the interruption of business activities lasting at least eight hours. An example of such a situation, as provided in the scope of insurance, is the case where the vessel will not be able to be steered due to the interruption of access to electronic navigational charts. Another product that can be mentioned is CyNav insurance, intended to cover marine cyber risks, which also covers damage to vessels and machinery as a result of a cyber attack[92]. Given its size and geographical location of the UK, the insurance market in the United Kingdom is able to provide significantly more specific products in the field of cyber transport insurance than is the case in the Czech Republic.

British insurers have very precisely defined policy exemptions to prevent unfounded claims and related disputes. Some conditions are surprising and that's why policy-holder should read insurance terms precisely. Aviva insurance limited will not cover insured person for more than one claim arising out form the same cyber extortionist.[93] Markel will not pay a claim arising out of the data liability or cyber liability, where the claim is brought in a court of law outside the jurisdiction of the applicable courts shown in the policy schedule, and/or, where action for damages is brought in a court within that jurisdiction to enforce a foreign judgment.[94] Some insurers exclude in the United Kingdom from

[90] Integrated Crime Cyberinsurance for Marine Transport Industry. Available from: https://www.shoreline.bm/downloads/ICCI-Product-Info-Sheet.pdf?v=1585231040 [Accessed 4 January 2021].

[91] Shoreline Ltd is seated in Hamilton, Bermuda. Bermuda is one of United Kingdom's overseas territories, and is therefore included in this insurance coverage comparison. In addition, the insurer is Maritime Insurance Solutions, which is reinsured by Lloyd's.

[92] *CyNav*. (2020) Navigating shipowners' cybersecurity risks. Available from: https://www.willistowerswatson.com/en-GB/Solutions/products/cynav-navigating-your-cyber-security-risks [Accessed 4 January 2021].

[93] Aviva Insurance Limited, Your insurance policy, version BCOAG 15628 (V36) 02.2021, p. 5.

[94] Markel UK Limited, Cyber and data risks, version CDR122016, p. 4.

the insurance cover terrorism, but they offer supplementary insurance based on specific conditions.[95]

3.5. PARTIAL CONCLUSION

Based on the analysis carried out in the practical part, it was found that cyber risk insurance in international transport is a non-life loss insurance, and may include property insurance (e.g. damage related to network security breaches, network outages, hacker attacks, or cyber extortion), legal expenses insurance (legal representation in proceedings relating to damage or other harm caused by a cyber attack) and liability insurance (breach of privacy, confidential information and personal data; media liability). In the cyber risk insurance area, there exists a close connection with the regulation governing the protection of personal and sensitive data according to Act No. 110/2019 Coll., on the processing of personal data and on amending certain laws, and Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of the personal data of individuals with regard to the processing of personal data and on the free movement of such data and repealing of Regulation (EC) 95/46 (General Data Protection Regulation)[96], as cyber risk insurance also covers the unauthorised handling[97] of personal data by the insured and his subcontractors.

Based on a comparison of the content of the insurance conditions for Internet risk and cyber risk insurance, it was found that cyber risks insurance is usually taken out with entrepreneurs, and insurance companies have prepared separate conditions for this type of insurance. These contractual conditions for the property and liability insurance of entrepreneurs are modified for the purposes of international transport insurance.

The insurance of cyber risks offered by insurance companies in the Czech Republic is identical in their basic elements. The differences lie in the scope of insurance coverage. The limits of insurance indemnity are negotiated individually according to the needs of the policyholder or the insured. The scope of cyber risk insurance is similar in comparison

[95] NIG Cyber cover policy, version NIG101423/10/19, p. 9 and 25.

[96] Took effect on 25 May 2018.

[97] This may involve the unauthorised collection, management, storage, disposal or other processing of personal data. However, it must not be an intentional unauthorised collection of personal data or the intentional processing of personal data in violation of legal regulations.

with selected insurance conditions used by insurance companies operating in other countries.

4. CONCLUSIONS

The subject of the analysis carried out in the first part of the article was to define the risks that arise in connection with cyber attacks in the international transport of goods. The individual types of transport were interpreted, which were divided in terms of the means of transport used. In the theoretical part of this article, it was found that the subject of a cyber attack can be physical attacks on hardware as well as software. In the case of an attacker's physical intrusion into the perimeter within which means of transport and equipment are located, the attacker risks easier detection and detention, but in some cases these attacks allow for the easier and faster control or manipulation of the system under attack, to which the attacker's devices are permanently or temporarily connected. In this area, it is clearly evident that a great risk is posed not only by the lack of computer equipment security, but also the negligence or intentional actions of their operators. Another element of vulnerability that was identified is the possibility of transmitting a false signal, which allows you to manipulate the positioning and associated navigation equipment. Legislative measures in this area are not yet sufficient, which is the reason why international governmental and non-governmental organisations are seeking additional regulation. However, the documents of such legislative measures are usually legally non-binding, i.e. recommendatory in nature.

Legislation as well as resources drafted and made available by international organisations usually respond retrospectively to cyber risks that have already arisen.

The aim of the second part of the article was to answer the question of whether it is possible to reduce or eliminate the risks associated with cyber attacks by taking out insurance. In this case, the purpose of insurance is to transfer the risks associated with cyber attacks to the insurance company, which arises if the legal and insurance conditions are duly met. The most insurance contracts in this area are tailor-made for the policyholder. Transport companies are already under-insuring the goods they transported, because comprehensive insurance, which would pertain to the entire period of transport and cover the full value of the goods, is very expensive. Therefore, it will always depend

on the specific case as to what limits of insurance benefits and exclusions from insurance will be agreed upon. In the case of insuring other transport equipment against cyber attacks, it will sometimes be difficult to determine the optimal limits of indemnity and to set the corresponding amount of indemnity. The starting point for negotiating suitable insurance conditions may be accounting or an estimation of the amount of damage arising based on model cyber attacks. The final form of the insurance contract and the insurance conditions will therefore always be a compromise between the requirement for an adequate amount of indemnity in the event of an insured event and the price of insurance that the policyholder will pay to the insurer.

LIST OF REFERENCES

[1] AIG. (2020) *Cyber Insurance Summarized Assessment Report, American International Group, Inc.* [online]. Available from: www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-summarized-assessment-report-sample.pdf [Accessed 24 June 2021].

[2] Author not specified. *Say hello to HMM Algericas, the largest container vessel on earth* , [online] Shipping and Freight Resource, [online]. Available from: https://www.shippingandfreightresource.com/hmm-algericas-largest-container-vessel-on earth [Accessed 15 October 2021].

[3] Barki, D. and Deleze-Black, L. (ed.) (2020) Developments in International Seaborn Trade. *UNCTAD Review of Maritime Transport* 2020.

[4] Barlatier, J. (2020) Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime. *Risks*, 8 (99), [online]. Available from https://doi.org/10.3390/risks8030099 [Accessed 23 June 2021].

[5] Bentley, M., Stephenson, A., Toscas, P., Zhu, Z. (2020) A Multivariate Model to Quantify and Mitigate Cybersecurity Risk, *Risks*, 8 (61), [online]. Available from https://doi.org/10.3390/risks8020061 [Accessed 24 June 2021].

[6] *BIMCO Guidelines on Cybersecurity Onboard Ships* (version 4, 2020).

[7] Burkacky, O., Deichmann, J., Klein, B., Pototzky, K., Scherf, G. (2020) *Cybersecurity in automotive: Mastering the challenge, report*, McKinsey&Company, [online]. Available from:www.mckinsey.com/industries/automotive-and-assembly/ourinsights/cybersecurit y-in-automotive-mastering-the-challenge# [Accessed 24 June 2021].

[8] Capra, G. S.: Protecting Critical Rail Infrastructure. The Counterproliferation Papers, *Future Warfare Series No. 38*, USAF Counterproliferation Center.

[9] CYRail Consortium Members. CYRail Recommendations on cybersecurity of rail signaling a communication systems. *UIC-ETF*, September 2018.

[10] Daily, J. et al. (2016) Towards a Cyber Assurance Testbed for Heavy Vehicle Electronic Controls. *SAE International Journal of Commercial Vehicles*, 9 (2).

[11] David, J. (2021) Cyber Attack on Railways in the Czech Republic. *Railtarget*, 22 March [online]. Available from: https://www.railtarget.eu/news/cyber-attack-on-railways-in-the-czech-republic-215.html [Accessed 24 June 2021].

[12] DiRenzo, J. et al. (2015) *The Little-known Challenge of Maritime Cybersecurity.* [online]. Available from: http://archive.dimacs.rutgers.edu/People/Staff/froberts/Maritime CyberCorfuPaper.final.pdf [Accessed 4 January 2021].

[13] Dobiáš, P. (2019) Kybernetická bezpečnost v mezinárodní přepravě se stále podceňuje, *Logistika* 25 (1).

[14] DPA/AFP.(2015) Hackers break into Lufthansa customer database. *Deutsche Welle,*10 April, [online]. Available from https://www.dw.com/en/hackers-break-into-lufthansa-customer-database/a-18374698 [Accessed 25 June 2021].

[15] Egan, R. et al. (2019) Cyber operational risk scenarios for insurance companies. *British Actuarial Journal,* 24, e6.

[16] EIOPA. Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies. *EIOPA*, 2. 8. 2018.

[17] Eling. M., McShane, M., Nguyen, T. (2021) Cyber risk management: History and future research directions. *Risk Management and Insurance Review,* 24, [online]. Available from: www.onlinelibrary.wiley.com/doi/epdf/10.1111/rmir.12169 [Accessed 25 June 2021].

[18] Forbes, V., L. (2018) *The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges.* [online]. Available from: www.futuredirections.org.au/publication/the-global-maritime-industry-remains-unprepared-for-future-cybersecurity-challenges/ [Accessed 4 January 2021].

[19] Goldbaum, Ch., Rashbaum, W. K. (2021) The M.T.A. Is Breached by Hackers as Cyberattacks Surge. *New York Times*, 2 June [online]. Available from: https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html [Accessed 24 June 2021].

[20] Goward, D. (2017) *Mass GPS Spoofing Attack in Black Sea?* [online]. Available from: www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea [Accessed 26 November 2021].

[21] Greenberg, A. (2016) Hackers Fool Tesla S'S Autopilot to Hide and Spoof Obstacles. [online] *New York: Wired.* Available from: www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles [Accessed 4 January 2021].

[22] Hahn, D., A., Munir, A., Behzadan, V. (2021) Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges, I*EEE Intell. Transp. Syst. Mag*., 13 (1).

[23] Hambling, D. (2017) Ships fooled GPS spoofing attack suggests Russian cyberweapon, *New Scientist* [online]. Available from: www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/ [Accessed 4 November 2021].

[24] Harvey, J., Kumar, S. (2020) *A Survey of Intelligent Transportation Systems Security: Challenges and Solutions, Conference paper*, May 2020, [online]. Available from: https://www.researchgate.net/publication/342405096 [Accessed 10 November 2021].

[25] IATA. *Situational Analysis, Introduction to Cybersecurity Threats, Cybersecurity Mitigation Practices, Setting Up a Management System, Risk Assessment and Prioritization Instructions*, 2nd edition, IATA, effective as of June 2015.

[26] IATA. *Compilation of Cybersecurity Regulations, Standards, and Guidance Applicable to Civil Aviation*, Edition 2.0, April 2021.

[27] ICAO Working paper, Assembly – 39 Session, Executive Committee, Agenda Item 16: *Aviation Security – Policy, Addressing Cybersecurity in Civil Aviation*, A39-WP/17 EX/5, 30. 5. 2016.

[28] ICAO, *Aviation Cybersecurity Strategy*, Quebec, October 2019, p. 2 – 4.

[29] ICAO Working paper, Assembly – 40 Session, Executive Committee, Agenda Item 12: *Aviation Security – Policy, ICAO Cybersecurity strategy*, A40-WP/28 EX/13, 25. 6. 2019.

[30] *IMO Guidelines on Maritime Cyber Risk management* (IMO's Maritime Safety Committee, MSC-FAL.1/Circular 3, 5. 7. 2017).

[31] Irwin, L. (2021) 2020 cyber security statistics, *IT Governance* [online]. Available from: www.itgovernance.co.uk/blog/2020-cyber-security-statistics [Accessed 24 June 2021].

[32] Jirásek, P., Novák, L., Požár, J. (2015) *Výkladový slovník kybernetické bezpečnosti,* Prague: PA CR in Prague, Czech branch of AFCEA.

[33] Jirovský, V. (2007) Kybernetická kriminalita. Prague: Grada.

[34] Karfíková, M. et al. (2018) *Insurance Law.* Prague: Leges.

[35] Kessler, G. C., Craiger, J. P., Haas, J. C. (2018) Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System, *TransNav*.

[36] Kilcarr, S. (2015) Battling a hack: One fleet's story. *Fort Atkinson: Fleetowner.* [online]. Available from: https://www.fleetowner.com/technology/article/21692058/battling-a-hack-one-fleets-story [Accessed 4 January 2021].

[37] Kolouch, J., Bašta, P. et al. (2019) Kybernetická bezpečnost. Prague: CZ.NIC.

[38] Kure, H. I., Islam, S., Razzaque, M. A. (2018) An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences,* 8 (6) [online]. Available from: www.mdpi.com/2076-3417/8/6/898 [Accessed 25 June 2021].

[39] Lévy-Bencheton, C., Darra, E. (2015) *Cybersecurity and Resilience of Intelligent Public Transport, Good practices and recommendations,* Athens: ENISA.

[40] MacGregor, L. (2019) British Airways faces largest ever data breach fine for 2018 hack. *New Scientist and Press Association.* 8 July. [online]. Available from: https://www.newscientist.com/article/2208964-british-airways-faces-largest-ever-data-breach-fine-for-2018-hack/ [Accessed 25 June 2021].

[41] Mearian, L. (2015) Firewalls can't protect today's connected cars, *Computerworld* [online]. Available from: www.computerworld.com/article/2951878/telematics/firewalls-cant-protect-todays-connected-cars.html [Accessed 4 January 2021].

[42] Mecheva, T., Kanakov, N. (2020) Cybersecurity in Intelligent Transportation Systems, *Computers,* 9, 83, p. 6-8 [online]. Available from: www.mdpi.com/journal/computers [Accessed 10 November 2021].

[43] Morán Blanco, M., S. (2017) La Ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. *Revista Española de Derecho International*, 69 (2).

[44] Muccin, E. (2015) *Combatting Maritime Cybersecurity Threats.* [online]. Available from: http://magazines.marinelink.com/Magazines/MaritimeReporter [Accessed 4 January 2021].

[45] Nurse, J., R., C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S. (2020) *The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes, Conference Paper,* p. 3 [online]. Available from: https://www.researchgate.net/publication/340849886_The_Data_that_Drives_Cyber_Insurance_A_Study_into_the_Underwriting_and_Claims_Processes/link/5f521074a6fdcc9879ca0a2d/download [Accessed 24 June 2021].

[46] Oxera. (2020) The value of cyber insurance to the UK economy, *Oxford: Oxera Consulting LLP*, [online]. Available from: www.oxera.com/insights/reports/the-value-of-cyber-insurance-to-the-uk-economy/ [Accessed 23 June 2021].

[47] Page, C. (2021) Air India Data Breach: Hackers Access Personal Details Of 4.5 Million Customers. *Forbes*, 23 May [online]. Available from: https://www.forbes.com/sites/carlypage/2021/05/23/air-india-data-breach-hackers-access-personal-details-of-45-million-customers/ [Accessed 25 June 2021].

[48] Quingley, K., Roy, J. (2011) Cyber-Security and Risk Management in an Interoperable World An Examination of Governmental Action in North America, *Social Science Computer Review.* 30 (1) [online]. Available from: http://ssc.sagepub.com/content/30/1/83 [Accessed 24 June 2021].

[49] Romanosky, S., Ablon, L., Kuehn, A., Jones, T. Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity,* 5 (1) [online]. Available from: https://doi.org/10.1093/cybsec/tyz002 [Accessed 23 June 2021].

[50] Saul, J. (2017): Global shipping feels fallout from Maersk cyber attack. [online] *Thomson Reuters.* Available from: https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE/ [Accessed 1 January 2021].

[51] Smejkal, V. (2018) *Kybernetická kriminalita*. 2nd ed. Pilsen: Aleš Čeněk.

[52] Svilicic, B., Brčić, D., Žuškin, S, Kalebić, D. (2019) Raising Awareness on Cyber Security of ECDIS, *TransNav*, 13 (1).

[53] Šulc, V. (2018) *Kybernetická bezpečnost.* Pilsen: Aleš Čeněk.

[54] The Nautical Institute. Charging your phone on the bridge? Think again!, *The Navigator,* June 2016.

[55] Tonn, G., Kesan, J. P., Czajkowski, J. and Zhang, L. (2018) *Cyber Risk and Insurance for Transportation Infrastructure*. [online]. Available from: https://riskcenter.wharton.upenn.edu/wp-content/uploads/2018/03/WP201802_Cyber-Security-Transportation-Sector.pdf [Accessed 4 January 2021].

[56] Ulianov, C., Hyde, P., Shaltout, R. E. (2018) Railway Applications for Monitoring and Tracking Systems. In: Marin Marinov (ed.) *Sustainable Rail Transport, Lecture Notes in Mobility*, Cham: Springer International Publishing.

[57] U. S. Department of Transportation. (2019) *Cybersecurity and Intelligent Transportation System, Best Practice Guide* – September 17, 2019, Publication Number: FHWA-JPO-19-

763, p. 35. [online] Available from: www.its.dot.gov/index.htm [Accessed 10 November 2021].

[58] Walker, J. (2018) *Autonomous Ships Timeline – Comparing Rolls-Royce, Kongsberg, Yara and More,* [online]. Available from: www.techemergence.com/autonomous-ships-timeline [Accessed 4 January 2021].

[59] Wares, S., Thompson, V. (2015) *Marsh Insights: Cyber Risk in the Transportation Industry,* p. 1, [online]. Available from: https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20Transportation%20Industry-03-2015.pdf [Accessed 4 January 2021]

[60] Weise, E. (2015) *Officials look into whether hacker really took over plane*. USA Today, 17 May. [online]. Available from: https://eu.usatoday.com/story/tech/2015/05/17/hacker-sideways-chris-roberts-fbi-united/27492409/ [Accessed 21 June 2021].

[61] Which. (2021) Popular connected cars from Ford and Volkswagen could put your security privacy and safety at risk, *Which? Finds, Which* [online]. Available from: https://press.which.co.uk/whichpressreleases/popular-connected-cars-from-ford-and-volkswagen-could-put-your-security-privacy-and-safety-at-risk-which-finds/ [Accessed 26 November 2021].

[62] Wrede, D., Stege, T., Graf von der Schulenburg, J.-M. (2020) Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. T*he Geneva papers on Risk and Insurance – Issues and Practice*, 45 (4) [online]. Available from: www.repo.uni-hannover.de/handle/123456789/10772 [Accessed 24 June 2021].