European Research Studies Journal
Volume XXVI, Issue 4, 2023

pp. 921-930

Maritime Industry Cybersecurity: A Review of Contemporary Threats

Submitted 25/10/23, 1st revision 12/11/23, 2nd revision 22/11/23, accepted 20/12/23

Adrianna Karaś[1]

Abstract:

Purpose: *This article aims to analyze the evolution of cyber threats in maritime transport, highlighting the increasing vulnerability of this sector to a variety of cyber attacks in the era of growing on advanced technologies.*
Design/Methodology/Approach: *The study employs a comprehensive literature review, analysis of industry reports, and data from real-world incidents related to cybersecurity in maritime transport.*
Findings: *The research identifies a range of cyber attacks affecting maritime transport, from phishing and ransomware to more sophisticated methods. It reveals that these cyber threats pose significant challenges to maritime safety. The study also highlights the evolving nature of these threats and the increasing sophistication of cyber attackers.*
Practical Implications: *Article underscores the need for enhanced awareness and preparedness among maritime professionals to mitigate the risks associated with these cyber threats.*
Originality/Value: *This article contributes to the existing body of knowledge by providing a detailed analysis of the diverse forms of cyber attacks in maritime transport and their implications. It offers valuable insights into the current state of maritime cybersecurity. The article highlights that cyber security in maritime transport is a critical aspect that requires constant attention and adaptation to rapidly changing threats.*

Keywords: *Cybersecurity, maritime industry, cyber threat, new technologies.*

JEL classification: *N70,R41, K24, Q55.*

Paper Type: *Review article.*

[1]*MSc, Gdynia Maritime University, Faculty of Management & Quality Science, Gdynia, Poland, a.karas@wznj.umg.edu.pl*

1. Introduction

Maritime transport, the core of global trade exchange, has evolved over centuries, adapting to dynamically changing economic, political, and technological conditions (Xu *et al.*, 2020; UNCTAD, 2021). The contemporary era of globalization, which has redefined the shape of international trade, has made maritime navigation essential for maintaining the continuity of global supply chains (Grzelakowski *et al.*, 2022; Zampeta and Chondrokoukis, 2022; 2023).

Technological advances have influenced the way the maritime industry operates today, and technological evolution in the maritime industry has brought enormous benefits and made maritime transport more efficient. Technologies such as remote cargo monitoring, advanced energy management systems, and automation of various onboard operations have made cargo transportation more efficient. These systems, based on real-time data, enable maritime enterprises to optimize routes, reduce emissions and maximize operational efficiency.

However, as in many other sectors, technological development has brought new challenges in terms of transport security (De Liso and Zamparini, 2022). Ships equipped with modern technologies become attractive targets for hackers, and even minor interference in ship navigation can lead to serious accidents, collisions, and threaten human safety (Akpan *et al.*, 2022).

Moreover, the maritime sector, including ports and terminals generates and processes vast amounts of data, which are attractive targets for cyber criminals. Information about transport routes, cargoes, and financial data can be used for criminal purposes (Visky *et al.*, 2022; Grima *et al.*, 2023).

Cyber security has become one of the most significant threats to the maritime industry today, with serious implications for its functioning (Naserinejad *et al.*, 2021). Cyber attacks on the maritime sector have become more advanced with increasingly severe consequences. Operational disruptions and theft of sensitive data can lead to significant financial losses (Punt *et al.*, 2023; McGillivary, 2018).

Therefore, understanding and managing cybersecurity in maritime transport is an important issue (Kapalidis, 2020). It is also important to note that cyberattacks can have various origins. They can be the result of actions by competing companies, third countries or even individual hackers. Motivations can vary - from industrial espionage, sabotage, to the desire to cause harm, and existing security measures often do not keep up with rapidly developing techniques of cybercriminals, requiring continuous updating and innovation in strategic management.

The importance of cyber security in maritime transport has been emphasized by numerous international and industry organizations, which have developed guidelines and standards aimed at minimizing risk (Muronga *et al.*, 2019).

However, despite these initiatives, the sector still faces challenges related to the continuous development of technology and the changing nature of cyber threats. Cyber security in maritime transport is not only a technological issue but also a strategic one. For many companies, investing in cybersecurity is an investment in their future, as well as a major challenge in the effective use of digital technology (Canepa *et al.*, 2021; Bartczak, 2021).

The article aims to examine the current state of cyber security in maritime transport, with an emphasis on the main threats and cyber attacks and their implications. Based on an analysis of scientific literature, data from actual incidents and industry reports, the article presents the complexity and essence of cyber security in the maritime industry.

2. Evolution of Cyber Threats in Maritime Transport and Technological Development

The evolution of cyber threats in the maritime sector shows a correlation with the dynamic technological progress and complexity of information systems. Initially, these threats were marginal and incidental, with attacks focusing mainly on simple malware and phishing techniques. However, the increased complexity of management systems and digitization has made this sector more vulnerable to more advanced cyber attacks.

A significant turning point in the evolution was the attack on management systems in the Belgian port of Antwerp in 2013, where cyber criminals exploited security loopholes to facilitate drug smuggling, demonstrating the ability to manipulate physical port operations using cyber tools and how the Internet is used, where drug trafficking groups recruit hackers to carry out "custom" cyber attacks (BBC, 2013; Tam *et al.*, 2016).

This incident showed that cyber attacks are becoming more advanced and recent years have seen a significant increase in both the scale and complexity of cyber attacks on the maritime sector, which cyber criminals use to carry out attacks. Cyber attacks carried out in recent years indicate the need to develop advanced cyber security systems and continuous monitoring and adaptation to the dynamically changing threat environment, including necessary legal regulations at the international level.

Total elimination or minimization of cyber risk and vulnerability can be achieved by increasing cybersecurity in the organization (Cheung *et al.*, 2021). Moreover, enhancing cyber security requires actions taken across the entire sector, taking into account both technical aspects and the human factor, and cybersecurity awareness in the era of growing importance of the Internet and technology is crucial (Golebiowska *et al.*, 2021).

Contemporary maritime transport, being a key element of global trade exchange due to its growing economic importance, faces challenges related to ensuring cyber security in the face of increasing dependence on digital technologies. Technological development brings new tools, technologies and methods that significantly improve safety in this industry.

Technologies such as Blockchain and Digital twin offer new opportunities not only in terms of optimizing operations but primarily in terms of risk management and increasing security. These solutions are essential in providing comprehensive protection against the growing cyber threats in the maritime transport industry. Implementing technologies requires continuous updating and adaptation to the rapidly changing cybersecurity landscape.

One of the key technologies being implemented in the maritime industry is Blockchain technology, considered groundbreaking since the introduction of the Internet (PWCHK.com, 2016). Researcher Nir Kshetri in his studies analyzes the impact of Blockchain technology on supply chain management, including maritime transport.

The author emphasizes that Blockchain can significantly affect key management goals such as cost reduction, quality improvement, speed, reliability, sustainable development and especially in the context of cybersecurity, allows for risk reduction (Rasheed *et al.,* 2022). Digital twin also plays an important role among technologies. San and Kvamsdal (2022) in their study discuss the concept of "Digital twin" as a virtual copy of a physical asset, supported by data from sensors.

The authors point to the potential of Digital twins in forecasting, optimizing, monitoring and controlling maritime operations, which is important in the context of cyber security. The digital twin or more precisely its application, aims to enable "what-if" predictions resulting in precise risk assessment. The Digital twin can be subjected to system disruptions to conduct potential and unexpected scenarios and examine the system's response to disruptions and in case of detected threats, implement appropriate management strategies (Kshetri, 2018).

3. Types of Cyber Attacks in Maritime Industry

The internet is a tool whose use increases the risk of cyber attacks. Installing software, exchanging data, logging into systems, online banking operations, using data carriers – these are just a few examples of activities during which a cyber attack is possible.

The maritime industry is also not immune to incidents related to cyber security, which are increasingly occurring. Practitioners and scientists clearly state that the number of cyber attacks and cyber vulnerabilities in maritime supply chains will increase year by year (Afenyo *et al.,* 2023).

Phishing Attacks:
Phishing attacks in the maritime industry often use fake emails containing suspicious links, messages, and documents that appear to come from trusted sources. These attacks aim to extract confidential information, including login data – usernames and passwords, cargo information, transport routes, and employee data. Authors Alcaide and Llave (2020) discuss cybersecurity in the maritime sector, emphasizing the growing vulnerability to cyber attacks, including phishing. These attacks can also lead to financial fraud and even take control of ship systems or port management systems (Alcaide and Llave, 2020).

Watering Hole Attacks:
In a "watering hole" attack, hackers target a website frequently visited by a specific group of people. Hackers identify security gaps and cybersecurity vulnerabilities, then manipulate the site to deliver malware that exploits these weaknesses. Once breached, the attacker can introduce malicious code into the site, which is activated when a user visits the site. Attackers increasingly use "watering hole" tactics for espionage attacks in various industries, including shipping and logistics enterprises (The Record, 2023; National Cyber Security Centre, 2023).

Physical Infiltrations:
Physical infiltrations in the maritime industry may include unauthorized access to ships, ports, or other maritime facilities for the purpose of conducting cyber attacks. Such actions can lead to data theft, manipulation of navigational systems, or disruptions in the operation of critical infrastructure. Mirovic et al. in their research discuss the use of large data sets in the maritime industry, which can be a cause of significant cyber risk (Mirovic *et al.*, 2018).

Furthermore, the authors point out that any physical connection to networks or systems can be susceptible to hostile attacks, and reports sent from ship to shore and vice versa can be intercepted and manipulated. Physical infiltrations can also lead to the installation of malicious software or listening devices, increasing the risk of cyber attacks.

Cyberpiracy:
Maritime piracy, while often associated with physical attacks on ships, can also include cyber aspects, such as attacks on ships' communication systems or ports. Cyber pirates can exploit security vulnerabilities to steal data, disrupt operations or even take control of ships. Authors Vaněk *et al.* (2013) present a model of maritime traffic in piracy-affected waters, which is relevant to the analysis of cyber threats.

The simulation created by the authors includes a global trade traffic model using a voyage planning tool. Cyberpiracy as a major threat to maritime security and economy, costing the global economy an estimated $7 billion, can also include attacks on cargo management systems, which can lead to theft of goods (Vaněk *et al.*, 2013).

Ransomware:
Ransomware attacks in the maritime industry can lead to disruptions in the operations or operating systems of ports or marine terminals. The aim of this type of attack is to damage an IT system or server by 'hacking' into computers connected to the network. Wang *et al.* and co-authors (2019) in their paper discuss the impact of Blockchain technology on supply chains, which may be linked to the risk of ransomware attacks.

As the authors point out Blockchain offers an alternative way to manage data, and the technology provides a high degree of security (Wang *et al.*, 2019). Ransomware attacks can lead to operational paralysis, which can have serious consequences for global trade and logistics. The most common destabilising attack on the supply chain is container diversion, which requires knowledge of the supply chain and the detection of a security vulnerability to modify strategic information.

IBS (Integrated bridge system (IBS) Tampering:
Among the cyber attacks, it is worth highlighting those related to communications and navigation in the broadest sense, which include bridge systems, Automatic Identification System (AIS), Voyage Data Recorder (VDR), Automatic Radar Plotting (ARPA), GPS/GNSS systems and electronic ECIDS.

AIS Spoofing:
Automatic identification system (AIS) is a system used to enhance maritime safety by providing real-time information, and the installation of AIS systems on ships requires software to provide the data, which raises security issues. One threat is the falsification of the CPA (Closest Point of Approach) by simulating a possible collision with a vessel, which consequently triggers an alarm and takes the vessel off course, e.g. running aground. Other cyber attacks using AIS include falsifying weather forecasts, impersonating ships. (Trend Micro, 2014; Pawelski, 2023).

VDR Tampering:
Tampering with voyage data recorder (VDR) records can lead to falsification of voyage information, which can be used to conceal illegal activities or manipulate evidence in maritime accidents. Awan et al. (2019) in their paper discuss the vulnerability of digital components of integrated bridge systems (IBS), including the VDR, to cyber-attacks (Awan and Al Ghamdi, 2019). Manipulation of the VDR can also lead to inaccurate ship status reporting, which can affect marine accident investigations.

GPS/GNSS Jamming:
GPS signal jamming can lead to errors in navigation and vessel location. Such attacks can cause serious threats to the safety of navigation, especially for vessels relying on precision navigation. Awan and Al. Ghamdi (2019) also discuss GPS threats in the context of maritime cyber security. Cyber attacks on the GNSS system are also becoming common, making the system vulnerable to breaches. False

position information significantly increases the likelihood of dangerous collisions (Ben Farah *et al.*, 2022)

ECDIS Malware:
Malware attacking ECDIS (Electronic Chart Display and Information System) systems can lead to erroneous navigational information, compromising the safety of navigation. These attacks can result in the incorrect display of charts, courses or other critical navigational data, leading to collisions or other maritime accidents involving vessels. Between 2016 and 2021, 13 major cyber incidents affecting the maritime industry were reported, including ECDIS malware, GPS forgery, ransomware and a direct attack on a port (Akpan *et al.*, 2022).

Among the types of cyber attacks, there are also those related to attacks on Wi-Fi networks, management systems e.g., Port Community System, intra-company messaging between employees, applications, watering hole attacks or supply chain attacks called Supply Chain Compromise Attack, when hackers sometimes demand a ransom to restore systems.

The activities of cyber criminals can be divided into untargeted attacks - which seek cyber vulnerabilities and gaps - and targeted attacks - which target a specific company/ship/institution/operating system. An example of a targeted attack is the activities of the APT40 hacking group, which has been linked to a series of attacks on the maritime industry, including ships and ports. The aim of these attacks is often the theft of sensitive information or industrial espionage.

A 2019 report by FireEye (now Mandiant) described the activities of the APT40 group, pointing to a five-year series of attacks aimed at stealing secrets and intellectual property to bolster China's navy APT40 attacks are characterised by advanced cyber techniques such as exploiting vulnerabilities, phishing and other infiltration methods, indicating the high level of skills and resources of this group (Rahman and Loukaka, 2021; Mandiant, 2023).

This diversity in cyber-attack strategies highlights the need for a comprehensive approach to cyber-security in the maritime industry that takes into account protection against both broad, automated attacks and the more complex, targeted activities of hacking groups such as APT40.

4. Conclusions

According to the International Maritime Organisation (IMO), "maritime cyber risk refers to a measure of the extent to which a technological asset may be threatened by a potential circumstance or event that could result in operational or navigational safety failures as a result of damage, loss or compromise of information security or systems" (IMO, 2022). And while the IMO clearly defines what a maritime cyber risk is, technological developments, which have brought significant efficiency and

management benefits, have at the same time created the opportunity and space for new cyber risks and incidents. In this context, the maritime sector, a key component of the global supply chain, appears to be particularly vulnerable to cyber attacks.

According to consultancy Naval Dome, the number of cyber incidents is reaching record numbers. Since February 2020, there has been a 400% increase in attempted attacks, an increase that is linked to a growing number of malware, ransomware and phishing attacks attempting to exploit the COVID-19 pandemic.

According to consultancy Naval Dome, travel restrictions and the economic recession have affected the defence capabilities of businesses. In addition, many IT systems have become more vulnerable to attacks, especially older ones where security vulnerabilities are easy to find. In the first quarter of 2020, attacks on home office workers increased tenfold, and security software company McAfee reported that cloud-based cyber attacks increased by 630 per cent between January and April (The Maritime Executive, 2020).

In conclusion, the article highlights that cyber security in maritime transport is a critical aspect that requires constant attention and adaptation to rapidly changing threats. Technological developments, while bringing undoubted benefits to the efficiency of maritime operations, at the same time open new gateways for cyber attacks that can have serious consequences not only economically but also in terms of security.

The rise in cyber incidents highlights the need for increased awareness and better defence strategies, and investment in cutting-edge cyber security technologies and infrastructure is equally necessary to address the rapidly changing threat landscape in the maritime industry.

References:

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., Michaloliakos, M. 2022. Cybersecurity Challenges in the Maritime Sector. Networks, 2(1), 123-124. https://doi.org/10.3390/network2010009.

Awan, M.S.K., Al Ghamdi, M.A. 2019. Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS). J. Mar. Sci. Eng. 7, 350. https://doi.org/10.3390/jmse7100350.

Bartczak, K. 2021. Cybersecurity as the Main Challenge to the Effective Use of Digital Technology Platforms in E-Commerce. European Research Studies Journal, Volume XXIV, Issue 2B, 240-256.

BBC. 2013. https://www.bbc.com/news/world-europe-24539417.

Ben Farah, M.A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., Bellekens, X. 2022. Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. Information, 13, 22. https://doi.org/10.3390/info13010022.

Canepa, M., Ballini, F., Dalaklis, D., Vakili, S., Colmenares Hernandez, L.M. 2021. CR CyberMar as a Solution Path towards Cybersecurity Soundness in Maritime Logistics Domain. Transactions on Maritime Science, 10(01). https://doi.org/10.7225/toms.v10.n01.011.

Golebiowska, A., Jakubczak, W., Prokopowicz, D., Jakubczak, R. 2021. Cybersecurity of Business Intelligence Analytics Based on the Processing of Large Sets of Information with the Use of Sentiment Analysis and Big Data. European Research Studies Journal, Volume XXIV, Issue 4, 850-871.

Grima, S., Thalassinos, E.I, Cristea, M., Kadlubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital Transformation, Strategic Resilience, Cyber Security and Risk Management. Emerald Group Publishing.

Grzelakowski, A.S., Herdzik, J., Skiba, S. 2022. Maritime Shipping Decarbonization: Roadmap to Meet Zero-Emission Target in Shipping as a Link in the Global Supply Chains. Energies, 15(17), 6150. https://doi.org/10.3390/en15176150 p.1.

IMO. 2022. Maritime cyber risk.

Ignacio Alcaide, J., Garcia Llave, R. 2020. Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, Vol. 45, 547-554. https://doi.org/10.1016/j.trpro.2020.03.058.

Kam-Fung, Ch., Bell, M.G.H., Bhattacharjya, J. 2021. Cybersecurity in logistics and supply chain management: An overview and future research directions. Transportation Research Part E: Logistics and Transportation Review, Vol. 146. https://doi.org/10.1016/j.tre.2020.102217.

Kapalidis, P. 2020. Cybersecurity at Sea. Global Challenges in Maritime Security. https://doi.org/10.1007/978-3-030-34630-0_8.

MANDIANT. 2023. https://www.mandiant.com/resources/blog/apt40-examining-a-china-nexus-espionage-actor.

Mawuli, A., Caesar, L.D. 2023. Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, Vol. 236. https://doi.org/10.1016/j.ocecoaman.2023.106493.

McGillivary, P. 2018. Why Maritime Cybersecurity Is an Ocean Policy Priority and How It Can Be Addressed. Marine Technology Society Journal, Vol. 52, No 5, 44. https://doi.org/10.4031/MTSJ.52.5.11.

Mirovic, M., Milicevic, M., Obradovic, I. 2018. Big Data in the Maritime Industry. Nase More, 65. https://doi.org/10.17818/NM/2018/1.8.

Muronga, K., Letebele, M., Binda, P., Smith S. 2019. Towards Secure Maritime Transport in South Africa: An Investigation of Cybersecurity Readiness of Organisations. In: 38th Southern African Transport Conference, Pretoria, CSIR ICC.

Naserinejad, A., Chebotareva, A., Chebotarev, V. 2021. Cyber security in marine transport: opportunities and legal challenges. Scientific Journal of Maritime Research, 35, 248-249. https://doi.org/10.31217/p.35.2.7.

National Cyber Security Centre. 2023. Supply chain security guidance. https://www.ncsc.gov.uk/collection/supply-chain-security/watering-hole-attacks.

De Liso, N., Zamparini, L. 2022. Innovation, transport security and supply chains: a review. TransportReviews, 42(6), 725. https://doi.org/10.1080/01441647.2022.2105415.

Kshetri, N. 2018. Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, Vol. 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005.

Vaněk, O., Jakob, M., Hrstka, O., Pěchouček, M. 2013. Agent-based model of maritime traffic in piracy-affected waters. Transportation Research Part C: Emerging Technologies, Vol. 36, 157-176. https://doi.org/10.1016/j.trc.2013.08.009.

Pawelski, J. 2023. Cyber Threats for Present and Future Commercial Shipping. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 17, No. 2, 261-267. https://doi:10.12716/1001.17.02.01.

Punt, E., Monstadt, J., Frank, S., Witte, P. 2023. Navigating cyber resilience in seaports: challenges of preparing for cyberattacks at the Port of Rotterdam, Digital Policy, Regulation and Governance, Vol. 25, No. 4, 429. https://doi.org/10.1108/DPRG-12-2022-0150.

PWCHK.com. 2016. Blockchain the Biggest Disruptor to Industries since the Introduction of the Internet– PwC. http://www.pwchk.com/home/eng/pr_070716.html.

Rahman, S.M.M., Loukaka, A. 2021. Security Professionals Must Reinforce Detect Attacks to Avoid Unauthorized Data Exposure. Information Technology in Industry, 8. https://doi.org/10.17762/itii.v8i1.76.

Rasheed, A., Omer, S., Kvamsdal, T. 2020. Digital Twin: Values, Challenges and Enablers From a Modeling Perspective. In: IEEE Access, vol. 8, 21980-22012. https://doi.org/10.1109/ACCESS.2020.2970143.

Tam, K., Kevin, J., Papadaki, M. 2016. Threats and Impacts in Maritime Cyber Security. Engineering & Technology Reference, 1. https://doi.org/10.1049/etr.2015.0123.

The Maritime Executive. 2020. https://maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent.

The Record. 2023. Suspected Iranian hackers target Israeli shipping and logistics companies. https://therecord.media/israel-shipping-logistics-watering-hole-cyberattacks.

Trend Micro. 2014. https://www.trendmicro.com/vinfo/it/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais.

UNCTAD. 2021. Review of Maritime Transport 2021. https://unctad.org/publication/review-maritime-transport-2021.

Xu, M., Pan, Q., Xia, H., Masuda, N. 2020 Estimating international trade status of countries from global liner shipping networks. Royal Society Open Science. https://doi.org/10.1098/rsos.200386.

Wang, Y., Hugh Han, J., Beynon-Davies, P. 2019. Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. Supply Chain Management: An International Journal, Vol. 24, Issue 1, 62-84. https://doi.org/10.1108/SCM-03-2018-0148.

Zampeta, V., Chondrokoukis, G. 2022. An Empirical Analysis for the Determination of Risk Factors of Work-Related Accidents in the Maritime Transportation Sector. Risks, 10(12), 231.

Zampeta, V., Chondrokoukis, G. 2023. A Comprehensive Approach through Robust Regression and Gaussian/Mixed-Markov Graphical Models on the Example of Maritime Transportation Accidents: Evidence from a Listed-in-NYSE Shipping Company. Journal of Risk and Financial Management, 16(3), 183.