ISSN 2524-101X
eISSN 2617-541X

DOI 10.62821/lp11101

Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures

Oleksiy Melnyk*, Oleksandr Drozdov**, Serhii Kuznichenko***

**Professor, Master Mariner, Navigation and Maritime Safety Department, Odesa National Maritime University (34, Mechnikova St., Odesa, Ukraine) https://orcid.org/0000-0001-9228-8459*

***Professor, Yaroslav Mudryi National Law University (77, Hryhoriia Skovorody St., Kharkiv, Ukraine), University of Barcelona (08034, 684 Av. Diagonal, Barcelona, Spain) https://orcid.org/0000-0003-1364-1272*

****Professor, National Academy of Legal Sciences of Ukraine (80, Chernyshevskaya St., Kharkiv, Ukraine) https://orcid.org/0000-0001-9278-2756*

ABSTRACT

This article combines legal, technical, and organizational aspects to propose a comprehensive approach to addressing cybersecurity of maritime transport. The article highlights key gaps in the international legal framework and suggests a unified legal framework to regulate these cyber threats from a maritime transportation perspective. The article focuses on technical solutions but is supported by professional training in a virtual environment. The main innovation of this article is the interdisciplinary approach, combining technological advances with social research and legal analysis. Among other proposals, developing an international maritime cybersecurity convention, a standard global incident registry and a transnational data sharing system are proposed. Such a systematic framework would have serious potential to address critical safety issues and improve the safety of the global shipping industry.

CITATION

Melnyk, O., Drozdov, O., & Kuznichenko, S. (2025). Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures. *Lex Portus*, *11*(1), 7–19. https://doi.org/10.62821/lp11101

KEYWORDS

maritime cybersecurity, maritime law, incident response, global maritime security standards, international legal frameworks

Introduction

Cyberthreats represents a vital concern for anything to do with global logistics and transportation security regarding the maritime industry. As shipping becomes largely dependent on digital technologies like automated vessel traffic management, IT systems, and electronic data exchange, it becomes more and more vulnerable to cyberattacks. Enacting legislation against these acts may represent a big step in the creation of an international maritime security configuration. However, several factors pose challenges to establishing law: the international character of maritime transport, the complicated identification, and the lack of uniform security standards.

Studies in recent times reveal that the maritime industry is becoming a victim of cyber-attack every year. Currently, vessel control systems, navigation systems, and logistics platforms are most frequently targeted by cyber perpetrators threatening the global maritime safety.

The gravity of cybersecurity issues in the maritime sector is well attested by academic studies like that of Emre et al. (2024), which details major cyber incidents within this realm, highlighting the inadequacy of ship control systems to guard against advanced attacks. A famous instance is the NotPetya virus, which altered the activities of Maersk and thus represents a far-reaching impact of cyberattacks on global supply chains.

According to Clavijo et al. (2024), maritime supply chains are especially vulnerable due to their multi-layer structure made of suppliers, transportation firms, and ports. Kanwal et al. (2022) pinpointed that current ship navigation systems (AIS, GPS) are poorly defended against cyber threats and, therefore, pose a significant threat to the security of the maritime domain. Further, Park et al. (2023) initiated an organized conclusion Failure Mode and Effects Analysis (FMEA) for risk evaluation; underlined the organization requirement under vulnerability evaluations within navigation systems. Progoulakis et al. (2022) presented cybersecurity issues in relation to port and offshore asset security threats, including essential security measures and collaborative defenses.

The analysis of port infrastructure was made difficult by the complexity within their cybersecurity by Syta (2024), who accentuated that many ports do not perform system modernization satisfactorily due to technological and financial constraints. Ports in developing countries remain extremely vulnerable, as emphasized and evidenced by Patrick et al. (2024), who discussed global port infrastructure protection practices with the C2M2 model as a case study. According to Sime (2023), many African ports remain vulnerable to threats because of the non-implementation of international standards into national legislation. Consequently, logistics losses would be significant and threaten disruption in global transportation.

Research confirms that cybersecurity threats in the maritime industry are growing, covering a wide range of issues. A review of the first decade of maritime cybersecurity research outlines key challenges and gaps in the field (Harish et al., 2025). The analysis of CO_2 emissions in maritime transport using AIS data demonstrates the importance of digital technologies for environmental monitoring, which is also a potential target for cyberattacks (Cheng et al., 2024). A bibliometric study of cybersecurity in the maritime sector over the past 20 years helps to identify the main research areas and prospects (Mawer et al., 2024). In matters of overall maritime security, it is important to consider both traditional and digital threats (Melnyk et al., 2022). The use of simulation modeling allows forecasting changes in maritime security under the influence of cyber threats and complex scenarios (Melnyk et al., 2023). In particular, the offshore oil and gas industry remains particularly vulnerable to attacks on remotely operated platforms and supply vessels, which poses additional challenges to the security of maritime operations (Progoulakis et al., 2021).

Countering cybercrime in maritime transportation calls for proper training of personnel. As such, Chupkemi & Mersinas (2024) submitted the need for compulsory cybersecurity training for shipping companies' employees. However, given the fast-changing threats, traditional training methods have become increasingly inadequate. According to Jepsen et al. (2024), a novel approach has been developed based on game-based learning, which better equips seafarers to become aware of the kinds of cyber-attacks they possibly face. Nikolov (2024) conceptualized a virtual training environment simulating real cyber threats while significantly improving operators' training aboard ships. Technology innovation is crucial in safeguarding maritime infrastructures. According to Ibokette et al. (2024), AI systems automatically detect network attacks, thus minimizing human error with regard to identifying such attacks.

A proposal to integrate sensor data into a single system to protect port infrastructure, allowing real-time monitoring of threats, Potamos et al. (2024) presented a proposal to integrate sensor data into a single system to protect port infrastructure, allowing real-time threat monitoring. Yousaf and Zhou (2024) also explored the possibility of using MITRE ATT&CK and D3FEND to protect ships, which they argue involves predicting upcoming attacks and responding automatically.

As noted by Martínez et al. (2024), such situation creates a disaggregated system of regulatory laws for cybersecurity in the maritime industry. This paper emphasizes the urgent need for

a binding international agreement governing the cybersecurity of any maritime infrastructure. Dimakopoulou and Rantos (2024) showed that linking maritime operations to international standards such as NIST CSF v2.0 proves that their adaptation can enhance ship security.

The cybersecurity is a key component of the modern maritime industry, as the digitalization of ports and vessels creates new threats (Neumann, 2024). A bibliometric analysis of current studies confirms that interest in this problem is emerging at a rapid pace (Peng et al., 2025; Mawer et al., 2024), and the main challenges remain unresolved.

A systematic review shows that cybersecurity threats include hacking of ship systems, attacks on automated ports, and risks to navigation (Bolbot et al., 2022). Text mining techniques are identifying new threats, especially in the transportation of dangerous goods (Huang et al., 2025). The risk life cycle of cargo ships is analyzed based on probabilistic models (Jiang et al., 2025). The development of risk assessment and mitigation methods is a priority for international organizations. For example, the CRAMMTS method allows assessing the cyber risks of maritime companies based on surveys (Tatar et al., 2024). Dynamic modeling of ship cyber resilience demonstrates the importance of a systematic approach (Putra et al., 2024). The level of employee awareness is a key factor in preventing cyber threats. An analysis of the level of knowledge of maritime students (Karaca & Soner, 2023) and industry workers (Aşan, 2024) revealed significant gaps. In Malaysia, the level of cybersecurity implementation depends on economic and regulatory factors (Ahmad et al., 2024). Big language models can be used to improve risk analysis and security of maritime operations (Miller et al., 2025). Automated approaches to risk and attack analysis can improve situational awareness (Xia et al., 2024). Research in Indonesia shows the effectiveness of a multi-level cyber defense strategy (Putri & Burhanuddin, 2023).

Autonomous vessels are particularly vulnerable to attacks on authentication systems (Crawford & Sylvanus, 2023). Legal aspects of gray areas in international maritime law affect cybersecurity law enforcement (Kormych et al., 2023). Military conflicts are changing the approach to maritime security, as the example of the Black Sea shows (Kormych et al., 2024). Risks in financial technologies and their connection with the maritime sector are studied in the context of digital transactions (Popova et al., 2024). An analysis of energy systems in maritime transport emphasizes the vulnerability to cyberattacks (Prasetyo et al., 2022).

The protection of ships in military convoys requires optimization of speed and schedule, which also affects overall security (Qiao et al., 2024). The use of eye-tracking technology allows to assess the level of attention of operators in critical situations (Petrović & Vujičić, 2025).

An analysis of the various works under review clearly reveals some gaps that require further investigation. Lack of a unified international legal framework, poor port security in developing countries, limited use of innovative technologies and low level of personnel training are the major gaps in combating cybercrime in maritime transportation. This article proposes to review applicable international and national legal frameworks, analyze the main technological measures to counter cyber threats and explore opportunities for international cooperation in this field.

1. Overview of cyber threats in shipping industry

The United Nations (UN), as well as the International Maritime Organization (IMO), have supported recommendations on maritime cyber security, as reflected in the adoption of resolution MSC.428(98). This resolution requires shipowners to include cyber risks in ship security management plans. However, at this point arose a jurisdiction problem since attacks can come from anywhere worldwide. Increased cooperation between states, intelligence sharing, and the creation of specialized cyber police units may be some ways to address the problem.

Cybersecurity in maritime transportation is a broad spectrum of threats targeting virtually all aspects of shipping and port infrastructure. For example, hacking into navigation systems, AIS or GPS, allows attackers to alter ship routes, create false coordinate positions, and cause collisions or cargo theft. Interference with vessel control systems, which takes control of onboard systems, leads to accidents, ship stoppages, or even hijackings. Stealing course data and cargo information - stealing important information about cargo in transit facilitates pirate attacks and economic blackmail. Sabotage against port systems is designed to paralyze port operations, from delayed unloading to mismanagement of containers, resulting in financial losses (Table 1).

Table 1. Classification of cyberattacks' targets in maritime transportation

Type of Target	Description	Possible Consequences
Navigation System Breach (AIS, GPS)	Interference with vessel navigation and communication systems	Route deviation, collision provocation
Ship Management System Interference	Hijacking vessel control, sabotaging onboard systems	Vessel hijacking, accidents, shipwrecks
Theft of Cargo and Route Data	Stealing commercial data on cargo and shipping routes	Financial losses, piracy
Sabotage of Port Operations	Breaching port management systems, delaying cargo handling	Logistics delays, financial losses

The history of shipping already knows many significant cyber incidents. One of the most famous cases was the NotPetya virus that paralyzed Maersk's global operations in 2017, causing an estimated $300 million in damages. The virus damaged corporate cargo management systems and caused disruptions at dozens of ports. Attacks on container terminals also pose a serious threat: in 2021, attackers disabled control systems at several major ports, causing huge delays. Lastly, cases of illegal intrusion into port systems include hackers who divert cargo, create false declarations or steal sensitive data, destabilizing global supply chains.

Various types of cyber threats affect maritime transport, including phishing attacks, malware infections, data breaches, ransomware, and DDoS attacks. The distribution of these threats is illustrated in Figure 1, based on cybersecurity reports analyzing maritime sector vulnerabilities.

Cyber threats can pose a real risk to shipping security, so their comprehensive classification is very important for countermeasures. Network attacks, such as distributed denial of service (DDoS) and man-in-the-middle (MITM), target communication systems, disrupt data flows, and jeopardize confidential exchanges. Malware such as viruses, Trojans, and spyware can damage critical systems and steal sensitive data.

Attacks on the security of navigation systems involve GPS spoofing and signal jamming. These actions manipulate ship location data, which disrupts navigation and jeopardizes operations. Cargo manipulation involves tampering with cargo or accompanying documents or altering shipment data, which can facilitate smuggling and illicit trade. Finally, social engineering is gaining access to critical maritime databases (Table 2) by exploiting weaknesses in the human factor through phishing or false login attempts.

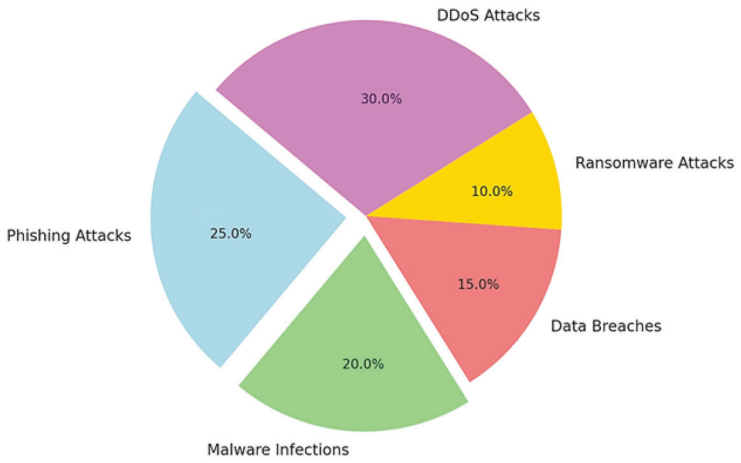

Figure 1. Distribution of cyber-attacks on maritime transport
(Source: Research analysis based on cybersecurity reports)

Table 2. Classification of cyber threats in the maritime industry

Category of Threats	Examples	Description
Network Attacks	DDoS, MITM, Phishing	Disruption of communication and data transfer
Malware Attacks	Viruses, Trojans, Spyware	System damage and data theft
Navigation System Attacks	GPS Spoofing, Signal Jamming	Ship disorientation and navigation failures
Cargo Manipulation	Cargo Data Forgery	Illegal operations and smuggling
Social Engineering	Phishing, Account Compromise	Hacking of personnel accounts through deception

Thus, the diagram in Figure 2 illustrates the complex mechanism of a cyber-attack on maritime transportation. It is structured to reflect both linear and branched attack paths, making it versatile for analyzing cyber threats in the maritime sector.

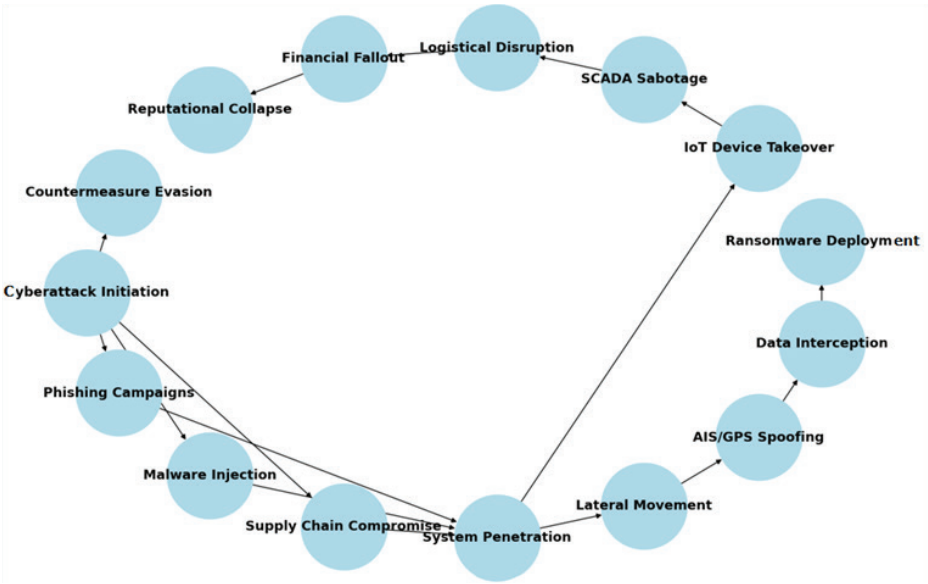

Figure 2. Compact Maritime Cyberattack Mechanism Diagram

The main nodes of the presented scheme include attack phases such as cyberattack initiation, hacking navigation systems, data collection, malware injection, and sabotage of port infrastructure. The cyberattack begins with vulnerable entry points, including phishing campaigns, malware injection, and supply chain compromise. Once infiltrated, attackers get to the system's vulnerabilities by navigating the network with elevated privileges.

Further steps include hacking into shipboard AIS/GPS systems, intercepting data, installing ransomware, and compromising IoT devices in port. All of this can lead to logistical disruptions, financial losses and resulting loss of reputation, as well as covert activities of attackers by masking their tracks and bypassing security systems.

2. Legal aspects of countering cyberthreats at sea

One of the key international instruments in the field of the law of the sea is the 1982 United Nations Convention on the Law of the Sea (UNCLOS), which establishes the foundations of the legal regime of the world's oceans. Although there are no explicit rules governing cybercrime in the text of the Convention, UNCLOS provides a framework for states to cooperate in ensuring the safety of maritime navigation and preventing unlawful acts. States are obliged to prevent the use of their ships for illegal activities, which can be interpreted as the need to counter cyber-attacks on ships flying their flag. It should be kept in mind that the legal framework of UNCLOS is limited to maritime cybersecurity applications, as the document initially focused on traditional threats such as piracy and illicit trade. However, the growing dependence of the maritime industry on digital technologies requires updating international treaties.

The Council of Europe Convention on Cybercrime (2001), known as the Budapest Convention, is the primary international agreement for combating cybercrime. While it initially focused on crimes committed on land, its principles can be adapted to the maritime domain. The Convention facilitates international cooperation, including extradition, joint investigations, and information exchange, which is vital given the global nature of cybercrime at sea.

According to IMO Resolution MSC.428(98), initiated by the International Maritime Organization (IMO), this regulation is the first to tackle maritime cybersecurity directly. It requires shipping companies to incorporate cyber risk management tools into their security management systems (ISM Code). This obligation aims to reduce the effects of cyber-attacks on vessels and diminish the risks to global maritime shipping.

National legal acts. These measures enacted by the leading maritime states are essentially the essential elements that make up the response to cybercrime in the maritime realm. The U.S. has passed an array of legal measures, such as the Maritime Transportation Security Act (MTSA) for the security of maritime transportation infrastructure and the Computer Fraud and Abuse Act (CFAA) addressing computer crime. These acts create a basis for protecting critical maritime infrastructure and legally punishing those who are perpetrating cyber-attacks.

In the European Union, the NIS (Network and Information Systems) Regulation was adopted and introduced mandatory cybersecurity standards for the operators of critical infrastructures, such as seaports and shipping companies. ENISA (European Cybersecurity Agency) is creating specific recommendations for the shipping industry to raise the level of protection of maritime systems. These measures, therefore, strengthen European legislation as adapted to address threats beyond maritime cyberattacks.

Jurisdiction and enforcement. Maritime cybercrime creates tremendous legal problems concerning jurisdiction and enforcement. The transnational nature of cyber-attacks

complicates the establishment of jurisdiction since some attacks may originate from servers in one state, affect vessels flying the flag of another, and impact the infrastructure of third countries. Jurisdiction for cyber-attacks against ships is determined by the flag under which they sail in accordance with UNCLOS, but such an approach is inadequate in the context of cyber threats.

Another difficulty regarding liability determination arises from issues in establishing the source of attacks. Legal scholars generally refer to the situation as "hybrid jurisdiction," according to which states conduct joint investigations into such incidents.

The collection and presentation of evidence are made even more difficult since the digital traces of cybercrime can be easily and quickly destroyed. Furthermore, international evidential procedures are stressed by each state's very different laws. In other words, the use of joint investigation teams and Mutual Legal Assistance Treaties (MLATs) becomes crucial in the whole process.

One of the prime issues in maritime cybersecurity concerns the ability to balance anonymity and identification in cyber-attacks. With the growing reliance on technologies such as IP masking and encrypted networks, identifying the perpetrator can be a case too thick to cut. Thus, new international frameworks on legal recognition of cyber-intelligence methods would go a long way in promoting data sharing among countries and between public and private sectors as possible solutions to the problem.

Legislation on maritime cybercrime should thus be related to international standards, national requirements, and stringent enforcement. International cooperation and the harmonization of legal standards across various countries would thus make a single international framework for the cybersecurity of maritime shipping possible.

3. Technological measures to counter maritime cyberthreats

Implementation of cyber security systems on ships and in ports. The development and implementation of technological solutions is a key element in countering maritime cyberthreats. These measures include security systems, cyber threat monitoring and standardization of management technologies. Effective cybersecurity systems protect ships and ports from cyberattacks. Modern systems include network infrastructure protection, data encryption, access control, and crew training. For example, the International Maritime Organization (IMO) recommends integrating cybersecurity into ship management systems to minimize the risks of attacks on navigation systems, automation and cargo platforms. Effective maritime defense requires comprehensive technical solutions, such as the use of automatic intrusion detection systems (IDS), cryptographic data transmission protocols, and firewalls with adaptive algorithms.

As shown in Figure 3, a hierarchical representation of the port cybersecurity system is used, using a branching structure to demonstrate the important components and their interrelationships. This emphasizes a layered approach to security measures, ranging from broad categories to detailed operational elements.

Artificial intelligence (AI) and machine learning systems can analyze large data sets in real-time and identify anomalies and suspicious activities. The application of AI makes it possible to predict potential threats, respond to incidents, and optimize ship management processes.

An important direction in ensuring maritime transportation safety is the creation of secure digital logistics platforms, such as global distribution systems (GDS) and passenger data management (PNR) platforms. These systems ensure the secure exchange of information between participants in the logistics chain, preventing data leaks and unauthorized access.

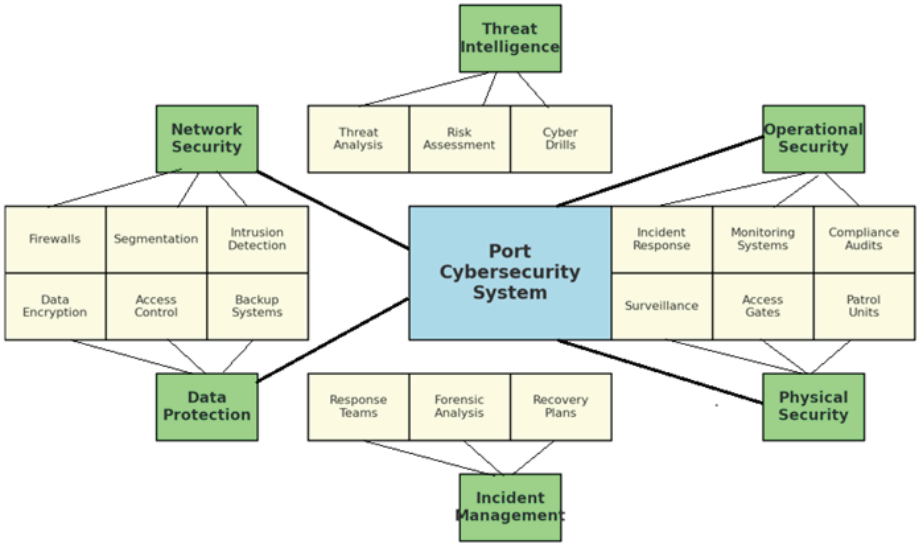

Figure 3. Hierarchical representation of the Port Cybersecurity System

Infrastructure projects. The introduction of autonomous ships has been an important step in the digitalization of the maritime industry. Remotely, captains operate autonomous ships using secure communication channels. These systems minimize the impact of human error and improve navigational safety. Examples of such projects include Rolls-Royce developments and the SEA-KIT autonomous ship project.

The diagram shown in Figure 4 depicts the interaction of key components of an autonomous control center used to coordinate the various elements in complex systems such as autonomous vessels.

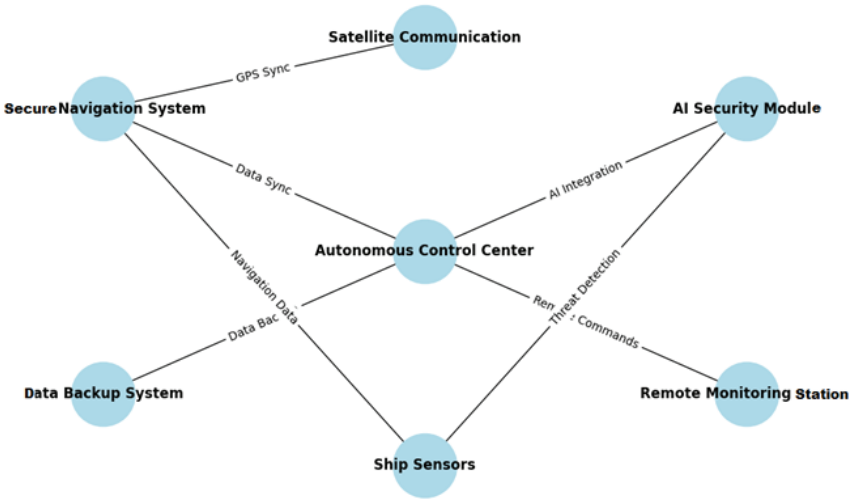

Figure 4. Advanced autonomous ship protection system architecture

The Autonomous Control Center is the core center, a control node that carries the relay of communication amongst the coalescing sensors, the navigation systems, safety modules, etc., other functional components. The interconnections between the elements illustrate very important data flows, for example, navigational information dissemination, threat detection, GPS synchronization, and redundancy of data. It takes care of the integrity and security of the system with the flexibility to go along with an intricate, real-time condition.

Indeed, ship management technology is set to be standardized, with all systems incorporating these standardized communications, navigation, and monitoring technologies. The International Maritime Organization strongly supports these standards, facilitating the integration of innovative technologies throughout the shipping industry. One notable initiative is the International SMART Ship project, which has emerged as a successful example of developing smart ships that enhance navigation capabilities and improve resilience against cyber threats.

Therefore, technological measures to eliminate cybercrime at seas involve protecting networks and data and establishing innovative solutions to secure the maritime infrastructure. The integration of standards, the use of AI, and the future advancement of autonomous vessels create a multi-tiered protective layer as our environment becomes more digital.

4. Organizational measures and international cooperation to counter syberthreats at sea

Combating cybercrime at sea requires coordinated action at the international level. Organizational measures include establishing international bodies, strengthening interstate cooperation, and developing training and certification for maritime professionals.

The International Maritime Organization (IMO) actively promotes maritime cyber security by establishing a special task force to develop policies, standards and recommendations. IMO Resolution MSC.428(98) requires shipowners to incorporate cyber risk management into ship security management systems, making this measure mandatory from 2021 onwards.

A number of international organizations and regional blocs, such as the European Union (EU) and the Shanghai Cooperation Organization (SCO), have entered into agreements aimed at coordinating efforts to secure digital infrastructure at sea. Examples include the EU's Network and Information Security (NIS) Directive and INTERPOL's global cooperation program to combat cybercrime.

To effectively address cyber threats, a dependable system whereby countries can exchange information regarding attacks, vulnerabilities, and best practices must be established. Organizations like Europol's EC3 and Interpol's International Cyber Defense Center help to facilitate rapid responses using worldwide early warning systems and joint research programs. An example of a successful international collaboration is the European Maritime Security Network (EMSA), uniting European states in countering and investigating cyberattacks.

The formation of joint incident investigation teams at the international level accelerates the detection of cyber-attacks on ships and maritime infrastructure. Examples of successful initiatives include INTERPOL's Operation OPERATION 404, which addresses cyber threats in international waters.

The cyber security competency of maritime industry professionals plays a key role in protecting ships. International training programs include courses on cyber risk management, cyber attack simulation and certification of maritime operators. Standards for cybersecurity training should be harmonized. International associations of maritime universities are developing training programs that are consistent with IMO and International Association of Maritime Institutes (IAMU) recommendations. Examples include international cybersecurity training at the IAMU in Sweden.

Thus, institutional measures, including the establishment of specialized bodies, interstate cooperation and the development of certification systems, play a crucial role in shaping a global strategy for preventing cybercrime at sea.

5. Discussion

Effectively countering cybercrime in the maritime industry requires a systematic approach that includes the development of international legislation, strengthening enforcement mechanisms and using advanced technologies. Let us consider the key areas of perspectives and recommendations.

Given the global nature of cybercrime, developing a specialized international convention regulating maritime cybersecurity is an urgent task. Such a convention could combine the norms of the International Convention for the Safety of Life at Sea (SOLAS), the United Nations Convention on the Law of the Sea (UNCLOS), and the Council of Europe Framework Convention on Cybercrime, ensuring more comprehensive regulation. Establishing an international maritime cyber threat data sharing system, including a global incident registry and a rapid response center, will enable rapid coordination of efforts.

Global sanctions mechanisms similar to those used for terrorism and piracy could be an effective deterrent. Such measures include asset freezes, a ban on maritime trade, and a ban on ships suspected of cyber-attacks entering ports of IMO member states.

A centralized database of cyber-attacks on ships and maritime facilities would improve threat monitoring by providing early warning of possible attacks. International organizations, such as IMO or INTERPOL, in cooperation with national authorities, could maintain this registry.

International rapid response teams for cyber-attacks could operate similarly to maritime rescue services. Such teams would conduct operational investigations, provide digital forensics, and protect key maritime assets from threats in real-time.

Blockchain technology can protect critical data such as navigation routes, ship logs and contracts. Blockchain-based systems can prevent information manipulation and ensure transparency and reliability of data in logistics chains.

Integrating autonomous cyber defense systems on ships will enable automatic detection and blocking of cyber-attacks. Artificial intelligence and machine learning will ensure constant monitoring of the ship's digital environment and the application of protective measures without human intervention. As mentioned, Rolls-Royce and Kongsberg are already developing examples of such systems.

Conclusions

The analysis of legal, technological and organizational aspects revealed such key challenges as the lack of a unified international regulatory framework, problems related to jurisdiction and attribution of cyberattacks, and the rapidly changing pace of development of technologies used by attackers. Key recommendations include developing a new international convention on maritime cybersecurity, implementing international mechanisms, creating global threat databases, and forming interstate task forces. Technological measures should be based on introducing autonomous defense systems, using blockchain for data protection and artificial intelligence for threat monitoring.

Legislation, technology, and training should be considered as part of a layered approach to finding solutions. Improved international cooperation, including information sharing and joint incident response, remains key to the security of the maritime industry. This argument points to an essential fact that the international community must realize global maritime cybersecurity standards must be developed to provide a robust, resilient framework to counter modern cyber threats. All proposed measures involve cooperation between states, maritime companies, and international organizations. In this way, global maritime cybersecurity standards will provide higher protection for shipping routes and ports, minimizing economic and social risks.

REFERENCES

Ahmad, N., Zainordin, N., Izni, N., Kahmin, A., & Shuen, Y. (2024). Factors affecting the cybersecurity adoption among players of the maritime industry, Malaysia. *International Journal of Advanced Research*, *12*, 633–640. https://doi.org/10.21474/IJAR01/19294

Aşan, C. (2024). Developing a measurement scale to assess the perception of cybersecurity among employees in the maritime industry. *Journal of Naval Sciences and Engineering*, *20*(2), 135–162. https://doi.org/10.56850/jnse.1485985

Bolbot, V., Kulkarni, K., Brunou, P., Valdez Banda, O., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, *39*, 100571. https://doi.org/10.1016/j.ijcip.2022.100571

Cheng, C., Li, Z., Yan, Y., Cui, Q., Zhang, Y., & Liu, Z. (2024). Maritime freight carbon emission in the U.S. using AIS data from 2018 to 2022. *Scientific Data*, *11*, 542. https://doi.org/10.1038/s41597-024-03391-0

Chupkemi, D., & Mersinas, K. (2024). Challenges in maritime cybersecurity training and compliance. *Journal of Marine Science and Engineering*, *12*(10), 1844. https://doi.org/10.3390/jmse12101844

Clavijo, V., Patino, C., & Guevara Carazas, F. (2024). Cybersecurity at sea: A literature review of cyber-attack impacts and defenses in maritime supply chains. *Information*, *15*(11), 710. https://doi.org/10.3390/info15110710

Computer Fraud and Abuse Act, 1986. U.S. Department of Justice. https://www.justice.gov/jm/jm-9-48000-computer-fraud

Convention on Cybercrime, 2001. Council of Europe. https://rm.coe.int/1680081561

Crawford, D., & Sylvanus, E. (2023). Enhancing cybersecurity in autonomous maritime systems: An analytical approach to system authentication. *Conference: Faculty of Computing and Applied Sciences International Conference on Sustainable Development Goals*, Baze University, Abuja.

Dimakopoulou, A., & Rantos, K. (2024). Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2.0. *Journal of Marine Science and Engineering*, *12*(6), 919. https://doi.org/10.3390/jmse12060919

Emre, D., Kayişoğlu, G., Acarer, T., Yilmaz Bolat, P., & Nak, A. (2024). Conducting an analysis of maritime cybersecurity incidents. *Turkish Journal of Maritime and Marine Sciences*, *10*(1), 51–61. https://doi.org/10.52998/trjmms.1531187

Harish, A. V., Tam, K., & Jones, K. (2025). Literature review of maritime cyber security: The first decade. *Maritime Technology and Research*, *7*(2), 273805. https://doi.org/10.33175/mtr.2025.273805

Huang, X., Wen, Y., Zhang, F., Li, H., Sui, Z., & Cheng, X. (2025). Accident analysis of waterway dangerous goods transport: Building an evolution network with text knowledge extraction. *Ocean Engineering*, *318*, 120176. https://doi.org/10.1016/j.oceaneng.2024.120176

Ibokette, A., Ogundare, T., Anyebe, A., Folami, O., Odeh, I., & Okafor, F. (2024). Mitigating maritime cybersecurity risks using AI-based intrusion detection systems and network automation during extreme environmental conditions. *International Journal of Scientific Research and Modern Technology*, *3*(10), 65–91. https://doi.org/10.38124/ijsrmt.v3i10.73

International Convention for the Safety of Life at Sea (SOLAS), 1974. International Maritime Organization. https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

International Maritime Organization. (2017, June 16). *Resolution on Maritime cyber risk management in safety management systems*. MSC.428(98). https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

Jepsen, L., Meland, P. H., & Kaloudi, N. (2024). Increasing maritime cybersecurity awareness through game-based learning. *Journal of Physics: Conference Series*, *2867*, 012050. https://doi.org/10.1088/1742-6596/2867/1/012050

Jiang, X., Xu, H., Zhu, Y., Gu, Y., & Zheng, S. (2025). Lifecycle risk assessment for steel cargo vessel sinkings: An interpretive structural modeling and fuzzy Bayesian network approach. *Journal of Marine Science and Engineering*, *13*(1), 165. https://doi.org/10.3390/jmse13010165

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C. (2022). Maritime cybersecurity: Are onboard systems ready? *Maritime Policy & Management*, *51*(3), 484–502. https://doi.org/10.1080/03088839.2022.2124464

Karaca, I., & Soner, O. (2023). An evaluation of students' cybersecurity awareness in the maritime industry. *International Journal of 3D Printing Technologies and Digital Industry*, *7*(1), 78–89. https://doi.org/10.46519/ij3dptdi.1236264

Kormych, B., Malyarenko, T., & Wittke, C. (2023). Rescaling the legal dimensions of grey zones: Evidence from Ukraine. *Global Policy*, *14*(3), 516–530. https://doi.org/10.1111/1758-5899.13233

Kormych, B., Averochkina, T., & Kormych, L. (2024). Black Sea, grain, and two humanitarian corridors: Unblocking Ukrainian shipping amid the Russian invasion. *Small Wars and Insurgencies*, *35*(8), 1360–1396. https://doi.org/10.1080/09592318.2024.2384679

Maritime transportation security act, 2002. Congress.gov. https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf

Martínez, F., Sánchez Crespo, L. E., Parra, A., Rosado, D., & Fernández-Medina, E. (2024). Maritime cybersecurity: Protecting digital seas. *International Journal of Information Security*, *23*, 1429–1457. https://doi.org/10.1007/s10207-023-00800-0

Mawer, T., von Solms, S., & Meyer, J. (2024). Identifying the scope of cybersecurity research conducted in the maritime industry: 2003–2023. *International Conference on Cyber Warfare and Security*, *19*(1), 545–554. https://doi.org/10.34190/iccws.19.1.2037

Melnyk, O., Onyshchenko, S., Lohinov, O., Ocheretna, V., & Dovidenko, Y. (2022). Basic aspects ensuring shipping safety. *Scientific Journal of Silesian University of Technology. Series Transport*, *117*, 139–149. https://doi.org/10.20858/sjsutst.2022.117.10

Melnyk, O., Onyshchenko, S., Onishchenko, O., Shcherbina, O., & Vasalatii, N. (2023). Simulation-based method for predicting changes in the ship's seaworthy condition under impact of various factors. In A. Zaporozhets (ed.) *Systems, Decision and Control in Energy V*. *Studies in Systems, Decision and Control*: Vol. 481 (pp. 653–664). Springer. https://doi.org/10.1007/978-3-031-35088-7_37

Miller, T., Durlik, I., Kostecka, E., Łobodzińska, A., Łazuga, K., & Kozlovska, P. (2025). Leveraging large language models for enhancing safety in maritime operations. *Applied Sciences (Switzerland)*, *15*(3), 1666. https://doi.org/10.3390/app15031666

Neumann, T. (2024). Cybersecurity in maritime industry. *TransNav*, *18*(4), 765–774. https://doi.org/10.12716/1001.18.04.02

Nikolov, B. (2024). Approach to developing a maritime cybersecurity virtual training environment. *Proceedings of the 15th International Scientific and Practical Conference "Environment. Technology. Resources":* Vol. *2* (pp. 220–225). https://doi.org/10.17770/etr2024vol2.8039

Park, C., Kontovas, C., Yang, Z., & Chang, C. (2023). A BN-driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, *235*, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

Patrick, M., Mugisha, E., Mbaga, K., & Likamba, M. (2024). Cybersecurity in Tanzanian maritime operations: Exploring global best practices and their local adaptation using the cybersecurity capability maturity model (C2M2). *Social Science and Humanities Journal*, *8*(10), 5688–5697. https://doi.org/10.18535/sshj.v8i10.1421

Peng, P., Xie, X., Claramunt, C., Lu, F., Gong, F., & Yan, R. (2025). Bibliometric analysis of maritime cybersecurity: Research status, focus, and perspectives. *Transportation Research Part E: Logistics and Transportation Review*, *195*, 103971. https://doi.org/10.1016/j.tre.2025.103971

Petrović, I., & Vujičić, S. (2025). Use of eye-tracking technology to determine differences between perceptual and actual navigational performance. *Journal of Marine Science and Engineering*, *13*(2), 247. https://doi.org/10.3390/jmse13020247

Popova, Y., Cernisevs, O., & Popovs, S. (2024). Impact of geographic location on risks of fintech as a representative of financial institutions. *Geographies*, *4*(4), 753–768. https://doi.org/10.3390/geographies4040041

Potamos, G., Stavrou, E., & Stavrou, S. (2024). Enhancing maritime cybersecurity through operational technology sensor data fusion: A comprehensive survey and analysis. *Sensors*, *24*(11), 3458. https://doi.org/10.3390/s24113458

Prasetyo, S. D., Prabowo, A. R., & Arifin, Z. (2022). The effect of collector design in increasing PVT performance: Current state and milestone. *Materials Today: Proceedings*, *63*, 1–9. https://doi.org/10.1016/j.matpr.2021.12.356

Progoulakis, I., Nikitakos, N., Rohmeyer, P., Bunin, B., Dalaklis, D., & Karamperidis, S. (2021). Perspectives on Cyber Security for Offshore Oil and Gas Assets. *Journal of Marine Science and Engineering*, *9*(2), 112. https://doi.org/10.3390/jmse9020112

Progoulakis, I., Nikitakos, N., Dalaklis, D., & Yaacob, R. (2022). Cyber-Physical Security for Ports Infrastructure. *International Maritime Transport and Logistics Conference*, *11*(1), 105–114. https://doi.org/10.21622/MARLOG.2022.11.105

Putra, I. N., Octavian, A., Susilo, A. K., & Santosa, Y. N. (2024). An assessment of cyber resilience in the maritime domain using system dynamics and analytical hierarchy process (AHP). *Transactions on Maritime Science*, *13*(2). https://doi.org/10.7225/toms.v13.n02.w06

Putri, S., & Burhanuddin, A. (2023). Maritime cybersecurity: Tantangan dan strategi keamanan maritim Indonesia. *Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora*, *2*(1), 378–386. https://doi.org/10.59059/mandub.v2i1.940

Qiao, X., Yang, Y., Jin, Y., & Wang, S. (2024**).** Joint ship scheduling and speed optimization for naval escort operations to ensure maritime security. *Journal of Marine Science and Engineering*, *12(8)*, 1454. https://doi.org/10.3390/jmse12081454

Sime, T. (2023). A critical reflection on African maritime cybersecurity frameworks. *Scientia Militaria*, *51*(3), 1–88. https://doi.org/10.5787/51-3-1426

Syta, J. (2024). Challenges in providing cybersecurity to port and maritime infrastructure facilities. *GIS Odyssey Journal*, *4*(1), 131–144. https://doi.org/10.57599/gisoj.2024.4.1.131

Tatar, U., Karabacak, B., Keskin, O. F., & Foti, D. P. (2024). Charting new waters with CRAMMTS: A survey-driven cybersecurity risk analysis method for maritime stakeholders. *Computers & Security*, *145*, 104015. https://doi.org/10.1016/j.cose.2024.104015

United Nations. (1982). *Convention on the Law of the Sea*. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

Xia, A., Guo, C., Li, S., Shen, Y., & Wang, Z. (2024). Research on network security situation prediction and visualization based on security situation awareness. *ACM International Conference Proceeding Series*, 287–293. https://doi.org/10.1145/3689236.3696754

Yousaf, A., & Zhou, J. (2024). From sinking to saving: MITRE ATT&CK and D3FEND frameworks for maritime cybersecurity. *International Journal of Information Security*, *23*, 1603–1618. https://doi.org/10.1007/s10207-024-00812-4

Мельник О., Дроздов О., Кузніченко С. Кібербезпека на морському транспорті: перспективи міжнародно-правового регулювання та заходи протидії. – Стаття.

У статті вивчено систему правових, технічних та організаційних заходів для формування комплексного підходу до вирішення проблеми кібербезпеки морського транспорту. Авторами висвітлено ключові прогалини у міжнародно-правовому регулюванні та пропонується створення єдиної правової бази у сфері кіберзагроз у морській транспортній сфері. Статтю сфокусовано на технічних рішеннях та підкріплено досвідом професійної підготовки у віртуальному середовищі. Інноваційним став застосований міждисциплінарний підхід, що поєднав технологічні досягнення з соціальними дослідженнями та правовим аналізом. Запропоновано розробку міжнародної конвенції з морської кібербезпеки, стандартизованого глобального реєстру інцидентів і транснаціональної системи обміну даними. Така системна база отримає вагомий потенціал для вирішення критичних безпекових проблем та підвищення безпеки світового судноплавства.

Ключові слова: морська кібербезпека, морське право, реагування на інциденти, глобальні стандарти морської безпеки, міжнародні правові засади.