DOI: https://doij.org/10.10000/IJLSI.112606

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 3

2025

Cybersecurity in Maritime Law: Legal Liability for Cyber-Attacks on Ships and Ports

SHLOK MHATRE[1] AND SHLOK MHATRE[2]

ABSTRACT

This research paper addresses the escalating cybersecurity risks in the maritime industry, driven by increasing reliance on digital systems for navigation, cargo management, and communication. It examines the types of cyberattacks targeting ships and ports, including GPS spoofing, ransomware, and communication system exploits, highlighting vulnerabilities in navigation systems, cargo management, and port infrastructure. The study explores the legal liabilities of shipowners, operators, and port authorities, focusing on duty of care, contractual obligations, regulatory compliance with IMO guidelines, and insurance considerations. It identifies gaps in the current international legal framework and jurisdictional complexities hindering effective enforcement. This paper emphasizes the need for a multi-faceted approach that includes harmonized global regulations, enhanced international cooperation, and proactive risk management strategies to safeguard maritime operations against evolving cyber threats.

I. INTRODUCTION

Cybersecurity in maritime law has become an increasingly critical concern as the shipping industry embraces digital technologies and interconnected systems. Modern vessels utilize complex computer systems for navigation, cargo management, and engine control. Similarly, ports employ digital infrastructure for logistics, customs processing, and security operations. While these advancements enhance efficiency, they also create potential entry points for malicious actors[3]. The rapid digitalization of ships and ports has brought numerous benefits, including improved efficiency, real-time tracking, and enhanced communication. However, this technological advancement has also exposed the maritime sector to new vulnerabilities and cyber threats. As a result, legal frameworks are evolving to address the complex issues surrounding legal liability for cyber attacks on ships and ports. The maritime industry, which handles approximately 90% of global trade[4], relies heavily on digital systems for navigation,

[1] Author is a student at Maharashtra National Law University Mumbai, India.
[2] Author is a student at Maharashtra National Law University Mumbai, India.
[3] Meixuan Li et al., Maritime Cybersecurity: A Comprehensive Review, Cornell University https://arxiv.org/abs/2409.11417.
[4] A Comprehensive Guide to Maritime Cybersecurity (2024).

cargo management, and communication. These systems, while essential for modern operations, create potential entry points for malicious actors seeking to exploit vulnerabilities[5].

Cyber attacks in the maritime domain can take various forms, including malware infections, denial-of-service attacks, and unauthorized access to sensitive data. The consequences of such incidents can be severe, ranging from financial losses and operational disruptions to environmental damage and threats to human life[6]. Cyber attacks on ships and ports can have severe consequences, ranging from financial losses and operational disruptions to environmental damage and threats to human life. Recent incidents have highlighted the urgency of addressing cybersecurity in maritime law. In 2017, the NotPetya malware attack affected Maersk, the world's largest container shipping company, causing an estimated $300 million in damages and disrupting global supply chains. Similarly, in 2020, the Mediterranean Shipping Company (MSC) experienced a network outage due to a cyber attack, impacting its operations worldwide[7]. These incidents underscore the need for robust legal frameworks to determine liability and ensure adequate protection against cyber threats.

The legal framework governing maritime cybersecurity is complex and evolving. International maritime laws and conventions, such as the International Convention for the Safety of Life at Sea (SOLAS) and the International Ship and Port Facility Security (ISPS) Code, provide a foundation for addressing security concerns. However, these instruments were primarily designed to address physical threats and require adaptation to encompass cyber risks adequately[8].

In response to the growing cyber threat, the International Maritime Organization (IMO) has taken steps to address cybersecurity. In 2017, the IMO adopted Resolution MSC.428(98), which encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems. Additionally, the IMO has issued guidelines on maritime cyber risk management, providing a framework for identifying, assessing, and mitigating cyber threats.

Determining legal liability for cyber attacks on ships and ports presents significant challenges. The transnational nature of maritime operations, involving multiple jurisdictions and

[5] Kimberly Tam & Kevin Jones, Maritime Cybersecurity Policy: The Scope and Impact of Evolving Technology on International Shipping, 3 Journal of Cyber Policy 147-164 (2018).

[6] Adrianna Karas, Maritime Industry Cybersecurity: A Review of Contemporary Threats, European Research Studies Journal 921-930 (2023).

[7] J Pawelski, Cyber Threats for Present and Future Commercial Shipping, 17 TransNav, the International Journal on Navigation and Safety of Sea Transportation 261-267 (2023).

[8] Oretis Schinas & Daniel Metzger, Cyber-Seaworthiness: A Critical Review of Literature, 151 Marine Policy (2023).

stakeholders, complicates the attribution of responsibility[9]. Key questions arise regarding the allocation of liability among shipowners, operators, charterers, and other parties involved in maritime transactions.

Under traditional maritime law principles, shipowners have a duty to ensure the seaworthiness of their vessels. In the context of cybersecurity, this duty may extend to maintaining adequate cyber defenses and implementing appropriate risk management measures. Failure to do so could potentially result in liability for damages arising from a cyber incident. Similarly, port authorities and operators may face liability for cyber attacks that exploit vulnerabilities in their digital infrastructure. This could include claims related to cargo loss, delays, or environmental damage resulting from a cyber-induced disruption of port operations[10].

Insurance plays a crucial role in managing cyber risks in the maritime sector. However, traditional marine insurance policies often exclude or limit coverage for cyber-related incidents. This has led to the development of specialized cyber insurance products tailored to the maritime industry's needs.

As the legal landscape continues to evolve, courts and arbitrators will likely play a significant role in shaping the interpretation of existing maritime laws and contracts in the context of cyber incidents. Future cases may establish precedents for determining liability and assessing damages in maritime cyber attack scenarios.

To address the challenges posed by maritime cyber threats, a multi-faceted approach is necessary[11]. This includes strengthening international legal frameworks, enhancing cooperation between states and industry stakeholders, and promoting the adoption of best practices in maritime cybersecurity. As technology continues to advance, the legal framework governing maritime cybersecurity must adapt to ensure adequate protection for ships, ports, and the global supply chain.

II. Cyber attacks on ships and ports: types, vulnerabilities and impacts

A cyberattack is a deliberate attempt by cybercriminals, hackers, or other malicious actors to infiltrate computer systems or networks with the intent to steal, alter, destroy, or expose

[9] Victor Bolbot et al., Developments and Research Directions in Maritime Cybersecurity: A Systematic Literature Review and Bibliometric Analysis, 39 International Journal of Critical Infrastructure Protection (2022).

[10] Ivan Mrakovic & Ranko Vojinovic, Maritime Cyber Security Analysis – How to Reduce Threats?, 8 Transactions on Maritime Science (2019).

[11] Joseph Chukwunweike et al., Enhancing Maritime Security Through Emerging Technologies:TheRole of Machine Learning in Cyber Threat Detection andMitigation, 5 International Journal of Research PublicationandReviews (2024).

sensitive information[12]. These attacks exploit vulnerabilities in digital infrastructure and can target individuals, organizations, or governments. Cyberattacks often compromise the confidentiality, integrity, or availability of data and systems, making them a growing threat in an increasingly interconnected world. Cyberattacks on ships and ports have become a critical concern as the maritime industry increasingly relies on digital systems. These attacks exploit vulnerabilities in navigation systems, cargo management, communication networks, and port infrastructure, causing significant operational, financial, and safety impacts.

Types of Cyber Attacks on Ships and Ports

1. Attacks on Navigation Systems[13]

Navigation systems such as GPS, Electronic Chart Display and Information Systems (ECDIS), and Automatic Identification Systems (AIS) are essential for ship operations but are highly vulnerable to cyber threats.

a. GPS Spoofing: Attackers manipulate GPS signals to mislead navigation systems about a vessel's location or route. This can result in ships being misdirected, leading to collisions or grounding incidents.

b. Malware in ECDIS: ECDIS often runs outdated operating systems like Windows XP, making it susceptible to malware introduced through USB drives or network access. For instance, malware can alter navigation charts or crash the system entirely.

c. AIS Manipulation: AIS signals can be spoofed to create phantom vessels or hide real ones, potentially facilitating smuggling or piracy.

Strategies Used:

a. Exploiting unencrypted communication protocols like NMEA 0183/2000.

b. Delivering malware via physical devices (e.g., USB) or phishing emails.

c. Conducting man-in-the-middle (MiTM) attacks to intercept and alter navigation data.

2. Attacks on Cargo Management Systems[14]

Cargo management systems are integral to port operations and onboard logistics, making them prime targets for cybercriminals.

[12] Joyce Hakmeh et al., What is a cyberattack?,Chatham House https://www.chathamhouse.org/2022/02/what-cyber-attack.

[13] Mohamed Amine Ben Farah et al., Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends, 13 Cyber Security for the Maritime Industry (2022).

[14] Bunyamin Gunes et al., Cyber Security Risk Assessment for Seaports: A Case Study of a Container Port, 103 Computers & Securities (2021).

a. Ransomware: Attackers encrypt critical cargo data and demand payment to restore access. The 2017 NotPetya attack disrupted Maersk's global operations, costing the company over $300 million[15].

b. Data Breaches: Hackers gain unauthorized access to cargo manifests, schedules, or personal crew information, which can be exploited for theft or smuggling.

c. System Manipulation: Criminals infiltrate cargo tracking systems to redirect specific containers. For example, hackers at Antwerp port accessed systems to steal drug-laden containers.

Strategies Used:

- Phishing emails targeting employees with access to cargo systems.

- Exploiting vulnerabilities in integrated IT-OT networks.

- Using compromised third-party software updates as entry points.

3. Attacks on Communication Systems[16]

Communication networks onboard ships and within ports are vital for coordination but are often poorly secured.

a. Satellite Communication Exploits: Vulnerabilities in marine Very Small Aperture Terminals (VSAT) allow attackers to eavesdrop on communications or inject malicious data[17].

b. Denial-of-Service (DoS) Attacks: Overloading communication networks with traffic renders them inoperable, disrupting ship-to-shore coordination[18].

c. Ballast Water Management System (BWMS) Hacks: Attackers manipulate ballast controls via network access, potentially destabilizing vessels.

Strategies Used:

a. Exploiting unencrypted satellite links and outdated communication protocols.

b. Using malware or phishing attacks to gain initial access.

c. Leveraging insider threats for physical access to communication devices.

[15] Chronis Kapalidis et al., A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships, 10 Journal of Marine Science and Engineering (2022).

[16] Oleksiy Polikarovskykh et al., Systematization of Cyber Threats in Maritime Transport, 1 Security of Infocommunication Systems and Internet of Things (2023).

[17] Imran Ashraf et al., A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry, 24 IEEE (2023).

[18] Boris svilicic et al., Towards a Cyber Secure Shipboard Radar, 73 The Journal of Navigation (2019).

4. Port Infrastructure Attacks[19]

Ports rely heavily on Operational Technology (OT) systems for cargo handling, access control, and overall management. These systems often lack robust cybersecurity measures.

a. Ransomware in Port Management Systems: Malware can lock down port operations entirely, as seen during the NotPetya attack.

b. Industrial Control System (ICS) Exploits: Hackers target cranes or fuel terminals controlled by legacy PLCs (Programmable Logic Controllers), causing operational disruptions.

c. Insider Threats: Disgruntled employees with access to sensitive systems may sabotage operations or leak credentials.

Strategies Used:

a. Exploiting weak network segmentation between administrative and operational systems.

b. Using brute-force attacks to compromise shared passwords.

c. Infiltrating supply chains via compromised hardware or software components.

The impacts of cyberattacks on ships and ports are far-reaching. Onboard ships, compromised navigation systems can endanger crew safety by causing collisions or grounding incidents[20]. Manipulated cargo management systems can lead to theft or loss of goods, while disruptions in communication can hinder emergency responses. In ports, cyberattacks can result in operational paralysis, financial losses due to downtime, and reputational damage. For example, Maersk incurred losses of over $300 million due to the NotPetya attack on its port operations[21]. Beyond economic consequences, cyberattacks on maritime infrastructure can also facilitate criminal activities like smuggling or drug trafficking by exploiting compromised tracking systems.

Addressing these vulnerabilities requires a comprehensive approach that includes regular updates to software and firmware, network segmentation to isolate critical systems from external threats, and robust access controls[22]. Collaboration between maritime authorities and cybersecurity experts is essential to develop resilient defenses against evolving threats in this

[19] Andrej Androja et al., Assessing Cyber Challenges of Maritime Navigation, 8 Journal of Marine Science and Engineering (2020).

[20] Andrew Tucci, Cyber Physical Security 113-131 (2016).

[21] Supra 12.

[22] Gabriel Weaver et al., Estimating Economic Losses From Cyber-Attacks on Shipping Ports: An Optimization-Based Approach, SSRN (2021).

domain. As the maritime industry continues its digital transformation, prioritizing cybersecurity will be crucial to safeguarding global trade and ensuring the safety of maritime operations[23].

III. Legal liability for shipowners, operators and port authorities in maritime cyber security

The maritime industry, reliant on complex digital systems for navigation, cargo management, and communication, faces significant legal liabilities in the event of cyberattacks. Shipowners, operators, and port authorities must navigate a complex web of contractual obligations, regulatory compliance, and potential negligence claims. This chapter explores the legal responsibilities and potential liabilities of these stakeholders in the context of maritime cybersecurity.

Duty of Care and Negligence

Shipowners and operators have a duty of care to ensure that their vessels are seaworthy and operated safely. This duty extends to maintaining robust cybersecurity measures to prevent and mitigate cyber threats. Failure to implement adequate cybersecurity protocols can lead to claims of negligence if a cyberattack results in damage or loss[24]. For instance, if a shipowner fails to update software or apply security patches, and this oversight leads to a successful cyberattack, they may be held liable for any resulting harm or financial losses.

Contractual Obligations

Contractual agreements between shipowners, operators, and charterers often include clauses related to cybersecurity[25]. The BIMCO Cyber Security Clause 2019, for example, requires parties to implement and review cybersecurity systems, ensure compliance by third-party service providers, and notify each other of incidents affecting cybersecurity. This clause also provides a default liability limit of $100,000 unless gross negligence or willful misconduct is proven[26]. Incorporating such clauses helps delineate and limit liability but requires adherence to specified cybersecurity standards.

[23] Kimberly Tam et al., Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety, 12 Journal of Transportation Technologies (2022).

[24] O metalla et al., Cyber Security in the Maritime Transport, Interdisciplinary Journal of Research and Development (2023).

[25] Daewon Kim et al., Potential Liability Issues of AI-Based Embedded Software in Maritime Autonomous Surface Ships for Maritime Safety in the Korean Maritime Industry, Journal of Marine Science and Engineering (2022).

[26] Supra 15.

Regulatory Compliance

The International Maritime Organization (IMO) has issued guidelines on maritime cyber risk management, emphasizing the integration of cybersecurity into existing Safety Management Systems (SMS) under the ISM Code[27]. Resolution MSC.428(98) encourages administrations to ensure that cyber risks are addressed in SMS by the first annual verification of a company's Document of Compliance after January 1, 2021. Compliance with these regulations is crucial for shipowners and operators to demonstrate due diligence in managing cyber risks.

Insurance Considerations[28]

Marine insurance policies often exclude cyber-related losses unless specific clauses are included. The LMA 5402 Marine Cyber Exclusion clause typically excludes coverage for cyberattacks intended to inflict harm, while the JCC Cyber Attack Exclusion Clause and Write-Back may provide some coverage under certain conditions. Shipowners and operators must carefully review their insurance policies to ensure they are adequately covered against cyber threats. However, given the limited coverage available, proactive cybersecurity measures remain essential[29].

Port Authorities' Liability[30]

Port authorities face liability risks related to the security of their infrastructure and operations. If a cyberattack compromises port systems, leading to operational disruptions or safety incidents, port authorities may be held liable for failing to maintain adequate cybersecurity standards[31]. This includes ensuring that third-party vendors and service providers adhere to robust cybersecurity practices to prevent supply chain attacks.

Mitigation Strategies

To mitigate legal liabilities, shipowners, operators, and port authorities should[32]:

1. Implement Robust Cybersecurity Measures: Regularly update software, use encryption, and segment networks to limit attack vectors.

2. Comply with Regulatory Guidelines: Adhere to IMO recommendations and incorporate

[27] Rory hopcraft & Keith M Martin, Effective Maritime Cybersecurity Regulation – The Case for a Cyber Code, 14 Journal of the Indian Ocean Region 354-366 (2018).

[28] Olga Karline Henkele, Unmanned Vessels: Liability and Insurance, Ghent University (2020).

[29] Baris Soyer, Maritime Law in Motion 627-642 (2024).

[30] Naserinejad Ali et al., Cyber Security in Marine Transport: Opportunities and Legal Challenges, (2021).

[31] Supra 11.

[32] Supra 21.

cybersecurity into SMS[33].

3. Incorporate Cyber security Clauses in Contracts: Use model clauses like BIMCO's to define responsibilities and limit liability.

4. Review Insurance Policies: Ensure adequate coverage for cyber-related risks.

5. Conduct Regular Risk Assessments: Identify vulnerabilities and address them proactively.

By adopting these strategies, stakeholders in the maritime industry can reduce their exposure to legal liabilities associated with cyberattacks and ensure safer, more resilient operations in an increasingly digital environment.

IV. JURISDICTION AND RISK MANAGEMENT IN MARITIME CYBER ATTACKS

The increasing reliance on digital systems in the maritime industry has exposed ships and ports to significant cyber threats. These attacks can disrupt operations, compromise sensitive data, and cause financial losses, raising critical concerns about jurisdiction and risk management. Jurisdiction in maritime cyberattacks is a multifaceted issue influenced by the location of the incident, the flag state of the vessel, and international maritime laws[34]. Determining jurisdiction often depends on several factors, including whether the attack occurs within a nation's territorial waters or on the high seas. If an attack happens within territorial waters (up to 12 nautical miles from the baseline), the nation has jurisdiction over the incident, applying its national laws governing cybersecurity, such as data protection regulations or criminal statutes.

On the high seas, jurisdiction is typically determined by the flag state of the affected vessel. Ships are subject to the laws of their flag state, as outlined in Article 92 of the United Nations Convention on the Law of the Sea (UNCLOS). Flag states are responsible for ensuring their vessels comply with international regulations, including cybersecurity standards like IMO Resolution MSC.428(98). This resolution requires shipowners and operators to integrate cyber risk management into their Safety Management Systems (SMS). However, cyberattacks often involve perpetrators operating across multiple jurisdictions, complicating enforcement and prosecution efforts[35]. Establishing the victim country is crucial for reporting incidents and facilitating international collaboration during investigations.

Effective risk management in maritime cybersecurity involves identifying vulnerabilities,

[33] Maritime cyber risk, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

[34] Omer soner et al., Risk Sensitivity Analysis of AIS Cyber Security Through Maritime Cyber Regulatory Frameworks, 142 Applied Ocean Research (2024).

[35] Maurantonio Caprolu et al., Vessels Cybersecurity: Issues, Challenges, and the Road Ahead, 58 IEEE Communications Magazine 90-96 (2020).

implementing protective measures, and preparing for incident response. Regulatory compliance is a cornerstone of risk management. Shipowners and operators must adhere to IMO guidelines, which mandate integrating cyber risk management into SMS. Additionally, the International Association of Classification Societies (IACS) has unified requirements that obligate shipbuilders and suppliers to incorporate cybersecurity barriers into onboard systems during design and construction phases[36]. Regional regulations, such as the EU Directive on Network and Information Systems (NIS2), also require operators of essential services like ports and shipping companies to adopt robust cybersecurity measures report serious incidents.

Developing comprehensive incident response plans is essential for mitigating damage during cyberattacks. This includes using advanced monitoring tools to detect anomalies in real-time and isolate affected systems, establishing procedures for restoring operations quickly while minimizing disruptions, and coordinating with national authorities, flag states, and international organizations during investigations[37]. Regular risk assessments help identify vulnerabilities in ship systems, such as AIS and ECDIS, and port infrastructure. Evaluating potential entry points for attackers, such as unencrypted communication channels or outdated software, and conducting penetration testing to simulate attacks and strengthen defenses are critical steps.

Insurance coverage is another important aspect of risk management. Cyber risks are increasingly being excluded from traditional marine insurance policies unless specific clauses are included. Therefore, it is crucial to review policies for coverage against ransomware attacks or data breaches and consider specialized cyber insurance products tailored to maritime operations. International collaboration is vital given the global nature of maritime operations. Sharing intelligence on emerging threats through organizations like INTERPOL or IMO and developing standardized reporting frameworks to streamline cross-border investigations are essential for effective risk management[38].

Despite robust regulatory frameworks, enforcing jurisdiction remains challenging due to attribution issues, legal gaps, and coordination barriers. Identifying perpetrators is difficult when attacks involve anonymized networks or multiple intermediaries. Many nations lack specific laws addressing maritime cybersecurity, and differences in national laws can hinder collaborative efforts during investigations. However, by adhering to international regulations,

[36] Victor Bolbot et al., A Novel Cyber-Risk Assessment Method for Ship Systems, 131 Safety Science (2020).

[37] Ivan mrakovic & Ranko Vojinovic, Maritime Cyber Security Analysis – How to Reduce Threats?, 8 Transactions on Maritime Sciences (2019).

[38] Suk Kyoon Kim, An Approach to Maritime Cyber Security Risks: Nature and Countermeasures, The International Journal of Marine and Coastal Law (2024).

conducting regular risk assessments, implementing incident response plans, and fostering global collaboration, shipowners, operators, and port authorities can mitigate risks effectively while navigating legal challenges associated with cyberattacks[39]. As digital transformation continues to reshape maritime operations, prioritizing cybersecurity will be essential for ensuring resilience across this critical industry.

V. Emerging legal issues and future challenges

The maritime industry's increasing reliance on digital systems has brought significant advancements in efficiency but also exposed it to a wide range of cyber threats. These threats pose not only operational and financial risks but also legal challenges that are rapidly evolving alongside technological advancements. This chapter explores emerging legal issues and future challenges in maritime cybersecurity, focusing on regulatory gaps, liability concerns, jurisdictional complexities, and the need for proactive risk management.

Emerging Legal Issues

1. Regulatory Gaps

The maritime sector faces a fragmented regulatory landscape when it comes to cybersecurity. While international frameworks such as the IMO Guidelines on Maritime Cyber Risk Management and the ISPS Code provide broad recommendations, they lack specificity in addressing emerging threats like ransomware, phishing, and advanced persistent threats (APTs)[40]. For instance, IMO Resolution MSC.428(98) mandates the integration of cyber risk management into Safety Management Systems (SMS), but enforcement varies across flag states. Additionally, regional regulations like the EU NIS2 Directive impose stricter requirements, including mandatory reporting of incidents within 24 hours, yet these rules are not uniformly applied worldwide.

The lack of harmonized global standards creates confusion about compliance obligations for shipowners, operators, and port authorities[41]. As technology evolves, new vulnerabilities emerge that are not adequately addressed by existing regulations. For example, the proliferation of Internet of Things (IoT) devices onboard ships introduces risks that current guidelines may not cover comprehensively.

[39] Matt Kuningas et al., Scenario 16: Cyber attacks against ships on the high seas, cyberlaw https://cyberlaw.ccdcoe.org/wiki/Scenario_16:_Cyber_attacks_against_ships_on_the_high_seas.

[40] Simone Fischer-H¨ubner et al., Stakeholder Perspectives and Requirements on Cybersecurity in Europe, 61 Journal of Information Security and Applications (2021).

[41] Fatih Durmaz, Cyber Risks on Autonomous Ships and Challenges in the International Law of the Sea, 16 European Journal of Commercial Contract Law (2024).

2. Liability Concerns

Determining liability in the event of a cyberattack remains a complex issue in maritime law. Shipowners and operators are often held responsible for ensuring the cybersecurity of their vessels under the principle of duty of care. However, questions arise when attacks exploit vulnerabilities in third-party systems or software suppliers[42]. For instance, if a ransomware attack targets a vessel through compromised software provided by an external vendor, liability may be shared or contested.

Contractual clauses like BIMCO's Cyber Security Clause 2019 attempt to allocate responsibility by requiring parties to implement cybersecurity measures and notify each other of incidents. However, these clauses often limit liability unless gross negligence or willful misconduct is proven. This creates challenges in attributing blame and recovering damages, especially when attacks involve sophisticated methods that make attribution difficult.

3. Jurisdictional Complexities

Cyberattacks often transcend national boundaries, complicating jurisdictional enforcement. Under UNCLOS Article 92, vessels on the high seas are subject to the laws of their flag state, but cyberattacks can originate from remote locations or involve servers across multiple jurisdictions. This raises questions about which nation has authority to investigate and prosecute such incidents.

Additionally, disputes may arise over whether an attack constitutes a breach of international law or merely a criminal act under national statutes[43]. For example, ransomware attacks targeting critical port infrastructure could be interpreted as acts of economic sabotage rather than conventional crimes. Resolving these jurisdictional dilemmas requires enhanced international cooperation and standardized reporting frameworks.

Future Challenges

1. Advanced Threats

The maritime sector faces increasingly sophisticated cyber threats such as ransomware with double extortion tactics, malware targeting operational technology (OT), and phishing campaigns exploiting human vulnerabilities. The integration of IoT devices and artificial intelligence (AI) into maritime systems further expands the attack surface for malicious actors.

[42] Chaomin Liu & Yuan Feng, Navigating Uncharted Waters: Legal Challenges and the Future of Unmanned Underwater Vehicles in Maritime Military Cyber Operations, 171 Marine Policy (2025).

[43] Konstantinos KOUROUPIS & Leonidas SOTIROPOULOS, Cyber Challenges Amid the Digital Revolution in Maritime Transport, Juridical Tribune - Review of Comparative and International Law (2024).

Emerging technologies like autonomous ships also pose unique risks that require new legal frameworks[44]. Autonomous vessels rely heavily on AI-driven navigation systems and remote monitoring, making them attractive targets for hackers seeking to disrupt operations or gain control over critical systems[45].

2. Supply Chain Vulnerabilities

Maritime cybersecurity is inherently linked to supply chain security. Attacks on ports or logistics providers can ripple through global trade networks, causing widespread disruptions. For example, ransomware attacks targeting port operators like DP World or Nagoya Port have demonstrated how cyber incidents can halt operations and impact entire economies[46].

Future challenges include securing interconnected supply chains against cascading effects of cyberattacks while addressing legal liabilities across multiple stakeholders involved in maritime logistics.

3. Insurance Limitations

Marine insurance policies often exclude coverage for cyber-related losses unless specific clauses are included. As cyberattacks grow more frequent and costly, insurers may impose stricter conditions or higher premiums for coverage. This creates financial challenges for shipowners and operators who must balance cybersecurity investments with rising insurance costs[47].

Recommendations

To address these emerging legal issues and future challenges:

1. Harmonize Global Regulations: Develop unified international standards that address advanced threats and ensure consistent enforcement across jurisdictions[48].

2. Strengthen Liability Frameworks: Clarify liability provisions in contracts and regulations to address third-party risks and shared responsibilities[49].

3. Enhance International Cooperation: Establish cross-border investigative protocols and

[44] Yonghyun Jo et al., Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework, 22 National Library of Medicine (2022).

[45] Nimra Tabish & Tsai Chaur-Luh, Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives, 12 IEEE Access 17114-17136 (2024).

[46] Konstantinos Kouroupis & Leonidas Sotiropoulos, Cyber Challenges Amid the Digital Revolution in Maritime Transport, Juridical Tribune - Review of Comparative and International Law (2024).

[47] Supra 21.

[48] Md Saiful Karim, Maritime Cybersecurity and the IMO Legal Instruments: Sluggish Response to an Escalating Threat?, 143 Marine Policy (2022).

[49] Wei Wang, Innovative Strategies and Forward Thinking on China’s Digital Maritime Law Enforcement, Marine Policy (2024).

intelligence-sharing mechanisms to tackle jurisdictional complexities.

4. Invest in Proactive Measures: Adopt advanced cybersecurity technologies such as AI-driven threat detection systems while conducting regular risk assessments.

5. Expand Insurance Coverage: Collaborate with insurers to create tailored policies that provide comprehensive protection against cyber risks[50].

Emerging legal issues and future challenges in maritime cybersecurity demand urgent attention as digital transformation reshapes the industry. By addressing regulatory gaps, liability concerns, jurisdictional complexities, and advanced threats proactively, stakeholders can build resilient systems that safeguard global trade while navigating an increasingly complex legal landscape.

VI. Conclusion

In conclusion, the rising tide of digital integration in the maritime industry, as explored in this research, presents both unprecedented opportunities and significant cybersecurity vulnerabilities that demand immediate and sustained attention. As modern vessels and port facilities increasingly rely on interconnected systems for navigation, cargo management, and communication, they inadvertently expose themselves to a diverse array of cyber threats. These threats, ranging from GPS spoofing and malware infections to ransomware attacks and data breaches, not only disrupt operations and cause substantial financial losses but also pose grave risks to human safety and the environment.

The patchwork of international maritime laws and conventions, while providing a foundational framework, struggles to keep pace with the rapidly evolving cyber landscape. The absence of harmonized global standards creates confusion and inconsistencies in compliance obligations, leaving critical gaps in protection. Determining legal liability in the aftermath of a cyberattack further complicates matters, with challenges arising from the transnational nature of maritime operations and the difficulty in attributing responsibility among various stakeholders.

To effectively address these challenges, a multi-faceted approach is essential. This includes strengthening international legal frameworks to create a more cohesive and comprehensive regulatory environment. Enhanced cooperation between states, industry stakeholders, and cybersecurity experts is paramount for sharing threat intelligence, developing best practices, and coordinating incident response efforts. Moreover, proactive risk management strategies, such as regular software updates, network segmentation, and robust access controls, are crucial

[50] Supra 36.

for mitigating vulnerabilities and minimizing the potential impact of cyberattacks. As the maritime industry continues its digital transformation, prioritizing cybersecurity will be critical for safeguarding global trade, ensuring the safety of maritime operations, and preserving the integrity of this vital sector.

*****