INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 6

2025

Ports, Protocols, and Perils: AI, IoT, and Cyber Risk in Maritime Operations

DAKSHA SHARMA*

ABSTRACT

The maritime sector forms the backbone of global trade, facilitating the movement of nearly 90% of international goods. As globalization accelerates, the shipping industry is adopting increasingly advanced digital technologies to improve efficiency and streamline operations. This transformation, however, has brought significant cybersecurity risks. The integration of operational and information technologies has spread and expanded vulnerabilities across vessels and port infrastructure, exposing the sector to a wide range of cyber threats. Cyberattacks on maritime systems can severely disrupt supply chains and compromise crew and cargo safety, resulting in substantial economic losses. Real-world incidents affecting major shipping companies and infrastructure show the growing scale and impact of such threats. In response, international and national bodies have developed frameworks and guidelines to encourage cyber risk management in maritime operations. Despite these efforts, serious underlying legal and jurisdictional challenges remain. The global and interconnected nature of maritime activities makes it exceedingly difficult to assign responsibility for cyber incidents. This study explores the gravity of cybersecurity risk and the vulnerability it poses to the current maritime regime. It also analyses the practices adopted by several developed and developing nations in safeguarding their maritime infrastructure. Finally, it proposes measures that need to be undertaken to strengthen the cybersecurity regime of the maritime sector.

Keywords: *Maritime cybersecurity, global trade, digital transformation, cyber risk, cyber insurance*

I. INTRODUCTION

The maritime sector stands as the backbone of global trade, facilitating the movement of approximately 90% of the world's cargo across oceans and waterways.[1] From the vast container ships that ferry goods between continents to the complex operations of port logistics, the maritime domain constitutes a crucial artery of the global economy.[2] With oceans covering more than 70% of the Earth's surface, maritime trade serves both as a facilitator of commerce and as one of the main enablers of energy distribution, supply chain resilience, and international

* Author is a Student at Narsee Monjee Institute of Management Studies (NMIMS), Hyderabad, Telangana, India.

[1] *Crucial Role of Shipping Agencies in Global Maritime Trade* (online article, undated).

[2] *Crucial Role of Shipping Agencies in Global Maritime Trade*, *supra* note 1.

 [ISSN 2581-9453]

development. Shipping agencies, shipowners, port authorities, and a complex web of other stakeholders collectively underpin this global network.[3]

Keeping this increasing significance in mind, the maritime industry has witnessed a technological renaissance of sorts, characterized by the rise of smart ports, automated vessels, and interconnected cyber-physical systems. The integration of operational technology (OT) and information technology (IT) has fundamentally transformed traditional maritime operations. Systems such as the Automatic Identification System (AIS), the Electronic Chart Display and Information System (ECDIS), Global Navigation Satellite Systems (GNSS), radio detection and ranging (RADAR), Very Small Aperture Terminals (VSAT), and the Voyage Data Recorder (VDR) are now essential parts of both ships and port infrastructure.[4] Recent surveys indicate that smart ports are leveraging IoT-enabled infrastructure, AI-based cargo management, blockchain for logistics integrity, and autonomous decision-making frameworks that streamline the entire process and maximize efficiency at the same time.[5]

However, the momentum of digital transformation has come with unprecedented risks. The growing reliance on technology has rendered the maritime sector extremely vulnerable to cybersecurity threats that were previously non-existent, or minimal, in an industry so long rooted in mechanical and analog systems. The convergence of IT and OT systems has expanded the attack surface, inviting new vectors of exploitation by nation-state actors, organized crime, and hacktivists alike.[6] These cyberattacks pose a tangible threat to the safety, security, and sustainability of maritime operations, with potential consequences including financial disruption, environmental disasters, and loss of human life.[7,8]

Cases such as the NotPetya ransomware attack on Maersk in 2017, which led to losses estimated at US$250 million to US$300 million, and MSC's network outage in 2020,[9] which disrupted its global logistics chain, underscore the sector's susceptibility to cyber incidents.[10] According to the United Kingdom's maritime cyber guidance, ransomware attacks on the maritime industry

[3] *Crucial Role of Shipping Agencies in Global Maritime Trade*, *supra* note 1.
[4] Meixuan Li et al., *Maritime Cybersecurity: A Comprehensive Review* (arXiv preprint No. 2409.11417, Nov. 6, 2024), https://arxiv.org/abs/2409.11417.
[5] *The Rise of Smart Ports: How Technology Is Revolutionizing Port Operations*, SHIP UNIVERSE (July 20, 2023), https://www.shipuniverse.com/the-rise-of-smart-ports-how-technology-is-revolutionizing-port-operations/.
[6] Li et al., *supra* note 4.
[7] S. Mhatre, *Cybersecurity in Maritime Law: Legal Liability for Cyber-Attacks on Ships and Ports*, 7 INT'L J. LEGAL SCI. & INNOVATION 85 (2025), https://ijlsi.com/wp-content/uploads/Cybersecurity-in-Maritime-Law.pdf.
[8] INTERNATIONAL MARITIME ORGANIZATION, *Maritime Security and Piracy*, https://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx (last visited Sept. 6, 2026).
[9] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[10] Mhatre, *supra* note 7.

rose by around 60% in 2022 compared with 2020, with at least fifty-seven known incidents reported in 2022 alone, most of them affecting IT systems through supply chain vulnerabilities.[11]

The International Maritime Organization (IMO) has responded to these threats by issuing key instruments, including Resolution MSC.428(98)[12] and MSC-FAL.1/Circ.3, which call for cyber risk management to be incorporated into safety management systems by 2021.[13] In the same way, classification societies such as the Indian Register of Shipping and industry groups such as BIMCO (the Baltic and International Maritime Council) have proposed frameworks to address cyber safety through notations, regular assessments, and cyber risk governance structures.[14]

Despite these regulatory and technical advances, the maritime sector continues to grapple with persistent and growing challenges that hinder its cybersecurity resilience. One major hurdle is the heterogeneity of shipboard systems, which vary widely in design, age, and integration capability, making it extremely difficult to implement unified security measures across fleets. This is compounded by the slow adoption of industry standards, which often lags behind the rapid pace of technological innovation, leaving critical systems exposed to growing threats. Additionally, human factors, more specifically the limited cyber awareness and training among seafarers, weaken the sector's defense posture even further. Complicating matters is the absence of globally harmonized legal regimes governing cyber liability and insurance, which creates uncertainty around accountability, compensation, and risk distribution in the aftermath of cyber incidents.[15] Together, these issues set up formidable obstacles to securing the increasingly digital maritime domain.

At the core of these vulnerabilities is the unique maritime cyber environment, marked by jurisdictional complexity, supply chain interdependencies, and legacy systems on board ships that were never designed to withstand modern cyber threats.[16] The dual nature of maritime

[11] DEPARTMENT FOR TRANSPORT & INSTITUTION OF ENGINEERING AND TECHNOLOGY, *Cyber Security Code of Practice for Ships* (July 2023), https://assets.publishing.service.gov.uk/media/64c929c0d8b1a71bd8b05e80/code-of-practice-cyber-security-for-ships.pdf.

[12] INTERNATIONAL MARITIME ORGANIZATION, Res. MSC.428(98), *Maritime Cyber Risk Management in Safety Management Systems* (adopted June 16, 2017), https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf.

[13] Res. MSC.428(98), *supra* note 12; INTERNATIONAL MARITIME ORGANIZATION, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3 (July 5, 2017), https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

[14] INDIAN REGISTER OF SHIPPING, *Guidelines on Maritime Cyber Safety* (Rev. 2, Aug. 2018), https://www.irclass.org/media/3849/guidelines-on-maritime-cyber-safety_new-version-rev2_06-aug-2018.pdf.

[15] Li et al., *supra* note 4.

[16] *Legal and Policy Issues with Maritime Cybersecurity* (undated).

systems, combining physical and virtual infrastructures, makes it difficult to apply conventional cybersecurity models without adaptation.

This paper explores the evolving cybersecurity landscape of the maritime sector, a critical artery of the global economy. As maritime trade undergoes a technological transformation marked by smart ports, automated vessels, and cyber-physical integration, the industry's operational backbone is becoming highly digitized and interconnected. The convergence of IT and OT has fundamentally changed maritime operations. Core systems such as AIS, ECDIS, GNSS, RADAR, VSAT, and VDR have enhanced efficiency, but they have also introduced new vulnerabilities in the cyber realm.

This integration has exponentially expanded the attack surface, making maritime assets both afloat and ashore susceptible to more numerous and more sophisticated cyber threats from state-sponsored actors, organized cybercriminal networks, and ideologically driven hackers. As the boundaries between IT and OT blur further, the risks to navigation safety, cargo integrity, and port operations have become increasingly tangible. These developments show the urgent need for comprehensive, resilient frameworks that combine legal, technical, and operational safeguards.

To address these challenges, the paper undertakes a cross-sectoral analysis of current cybersecurity practices, regulatory instruments, and real-world incidents affecting the maritime domain. It critically examines the effectiveness of existing cyber defense measures within ships and port infrastructure, identifies systemic vulnerabilities across IT and OT systems, and evaluates the adequacy of evolving legal and institutional frameworks. On this basis, it offers strategic recommendations to strengthen cyber resilience in the maritime sector, emphasizing risk-based governance, regulatory harmonization, and the deployment of advanced technological solutions. The end goal is to support the development of an adaptive and secure maritime ecosystem, capable of navigating the complex threats of an increasingly digitized world.

II. UNDERSTANDING MARITIME CYBERSECURITY

A. Definition and scope of cybersecurity in the maritime context

Maritime cybersecurity refers to the protection of IT and OT systems, as well as digital infrastructure, across vessels, ports, and maritime logistics chains. It comprises the defense of interconnected digital assets, from onboard ship systems such as navigation, propulsion, and communication networks to onshore operations such as cargo management and customs processing, against cyber threats that could compromise safety, security, environmental

integrity, and operational continuity. As vessels and ports increasingly rely on integrated cyber-physical systems such as AIS, ECDIS, GNSS, RADAR, VSAT, VDR, and the Global Maritime Distress and Safety System (GMDSS), the convergence of IT and OT expands the attack surface. This integration exposes formerly isolated systems to network-based vulnerabilities, making them more susceptible to malware, ransomware, data breaches, and system disruptions. Cyberattacks targeting maritime operations have increased, with a marked rise in incidents since 2020. Threat actors ranging from nation-states and criminal syndicates to hacktivists exploit these vulnerabilities for espionage, financial theft, or sabotage. Ports are especially attractive targets because of their involvement in high-value trade and their extensive digital interfaces. For instance, large-scale cyberattacks on European ports disrupted oil terminal operations, demonstrating the cascading impact of digital threats on global supply chains.[17]

According to the Indian Register of Shipping's Guidelines on Maritime Cyber Safety, cybersecurity consists of a comprehensive system of policies, training, physical and system access controls, asset management, detection, and recovery protocols aimed at mitigating cyber risk. These practices are enforced through classification notations and cyber safety surveys conducted regularly during a ship's lifecycle, from construction to operation.[18] The IMO emphasizes that ships' onboard IT and OT systems are just as vulnerable as land-based systems, and that failures could jeopardize lives, cargo, and even national economies. Accordingly, the IMO has issued Guidelines on Maritime Cyber Risk Management, requiring operators to incorporate cyber risk into their existing safety management systems under the ISM Code.[19] A holistic cybersecurity approach not only addresses technical hardening but also includes governance structures, awareness programs, and continuous process reviews to build a resilient and adaptive maritime ecosystem.[20,21] Beyond these technical safeguards, there is also a recognized need for harmonized legal and regulatory frameworks that facilitate reporting, prosecution, and transnational coordination to reduce cybercrime in the maritime domain.[22]

The IMO defines maritime cyber risk as a measure of the extent to which a technology asset could be threatened by a potential circumstance or event.[23] Such an event may lead to

[17] Giovanni Marchiafava, *Cybercrime and Cybersecurity in Shipping: A Legal Framework in Progress*, 89 RIVISTA DI STUDI POLITICI INTERNAZIONALI 239 (2022).
[18] INDIAN REGISTER OF SHIPPING, *supra* note 14.
[19] INTERNATIONAL MARITIME ORGANIZATION, *Maritime Cyber Risk*, https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx (last visited Sept. 6, 2026).
[20] BIMCO et al., *The Guidelines on Cyber Security Onboard Ships* (Version 4, Dec. 2020), https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf.
[21] Li et al., *supra* note 4.
[22] Marchiafava, *supra* note 17.
[23] INTERNATIONAL MARITIME ORGANIZATION, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3, at 1 (July 5, 2017),

operational disruptions, loss of confidentiality, data manipulation, or safety failures. This risk management framework was formally acknowledged with the adoption of Resolution MSC.428(98),[24] which affirms that safety management systems should account for cyber risks by integrating them into the International Safety Management (ISM) Code.

The scope of maritime cybersecurity now extends far beyond the confines of ships. It includes port control systems, cargo tracking software, satellite communications, vessel traffic systems, and administrative databases. Technologies such as ECDIS, AIS, GMDSS, and VSAT form part of a cyber-physical ecosystem whose disruption can have severe consequences. As digital transformation accelerates across maritime trade, the convergence of IT and OT makes cybersecurity a cornerstone of modern maritime safety. Maritime stakeholders, including shipping companies, port operators, customs agencies, and insurers, now operate within a highly digitized and interdependent environment. Consequently, cybersecurity has become both a technical necessity and a strategic imperative.

B. Types of cyber threats in the maritime sector

Cyber threats in the maritime context have grown in complexity and intensity, particularly as vessels and ports adopt artificial intelligence (AI), autonomous systems, and Internet of Things (IoT)-enabled platforms.

i. Traditional cyber threats

Traditional cyber threats in the maritime sector pose significant risks to vessel safety and operational integrity. Among the most prevalent are malware and ransomware attacks, which can infiltrate critical onboard systems such as ECDIS or bridge control mechanisms, potentially resulting in data corruption, system lockouts, or even manipulated navigational instructions. Phishing and social engineering tactics also present serious vulnerabilities, as cybercriminals target seafarers and shore-based personnel through deceptive emails or communications to gain unauthorized access to secure networks and sensitive data. Additionally, GPS spoofing and jamming have emerged as alarming threats, in which malicious actors compromise GNSS signals to distort vessel positioning, leading to navigational confusion or misdirection. Another critical risk is unauthorized remote access, often achieved by exploiting weaknesses in satellite communication systems such as VSAT. Such breaches can allow hackers to penetrate OT networks, potentially seizing control of vital shipboard functions from afar. Collectively, these

https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

[24] Res. MSC.428(98), *supra* note 12.

traditional cyber threats highlight the urgent need for robust, multilayered defenses within maritime cybersecurity frameworks.[25]

ii. AI-enabled threats

The integration of artificial intelligence into maritime operations, particularly in areas such as route optimization, predictive maintenance, and autonomous vessel control, has introduced a new class of sophisticated cyber threats. One such threat is data poisoning, where attackers deliberately manipulate the input data fed into AI models. This can lead to flawed decision-making on board, such as incorrect route planning, misidentification of nearby vessels, or failure to recognize navigational hazards. Another emerging concern is algorithmic attacks, which target the internal logic of AI systems to induce erratic or unsafe behavior. In contexts such as autonomous navigation or automated crane operations at ports, even minor disruptions in algorithmic functioning can cause severe safety and logistical consequences. Furthermore, the rise of deepfakes and synthetic identities poses a unique challenge in maritime cybersecurity. These technologies can be used to fabricate false identities or credentials, enabling unauthorized access to shipping management systems, crew databases, or cargo control software. Collectively, these AI-enabled threats highlight the growing complexity of securing maritime systems and the urgent need for proactive, AI-aware cybersecurity measures.[26]

iii. IoT and interconnected threats

The rapid proliferation of smart sensors, real-time tracking technologies, and interconnected control systems in modern maritime operations has significantly expanded the cyber threat landscape. These IoT devices, while enhancing efficiency and visibility across shipping and port logistics, also introduce numerous entry points for cyberattacks. A breach in a single IoT device or an unpatched software gateway can trigger cascading failures across the network, leading to widespread disruptions, from malfunctioning container tracking systems to the paralysis of automated port crane operations. Compounding this vulnerability is the increasing use of AI in cybersecurity defenses. While AI-powered intrusion detection systems offer advanced monitoring capabilities, they are not immune to adversarial techniques, in which sophisticated attackers study and manipulate the detection logic of these systems to avoid being flagged. This strategic evasion undermines the reliability of AI defenses and highlights the

[25] BIMCO et al., *supra* note 20.
[26] Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (Feb. 2018), https://arxiv.org/abs/1802.07228.

evolving sophistication of maritime cyber threats in an interconnected, intelligent maritime ecosystem.[27]

C. Real-world incidents demonstrating maritime cyber vulnerabilities

Numerous incidents over the last decade highlight the real and growing threat posed by cyberattacks in the maritime domain.

i. IMO cyberattack (2020)

In late September and early October 2020, the IMO itself suffered a cyberattack that took down its public website and web-based services.[28] As the regulatory authority for global shipping, the IMO's own vulnerability reflected the systemic risks facing maritime governance and information exchange frameworks.

ii. Maersk NotPetya attack (2017)

One of the best-known maritime cyber incidents was the NotPetya ransomware attack on A.P. Moller-Maersk.[29] The attack disrupted global shipping operations, froze port terminals, and led to estimated losses of US$250 million to US$300 million. The malware spread through Maersk's Ukrainian office and crippled critical business systems worldwide, halting vessel bookings and cargo movements.

iii. Port terminal attacks in Europe (2022)

In 2022, cyberattacks targeted multiple oil terminals in Belgium, the Netherlands, and Germany, disrupting operations and delaying tanker deliveries.[30] These attacks exploited vulnerabilities in port logistics software and highlighted how interconnected critical infrastructure can be paralyzed by cyber disruption.

---

[27] Brundage et al., *supra* note 26; Li et al., *supra* note 4.

[28] INTERNATIONAL MARITIME ORGANIZATION, *IMO Web Services: Update 02/10/2020, Access to the www.imo.org Website Restored* (Oct. 2, 2020), https://imo-newsroom.prgloo.com/news/imo-web-services-update-02102020; Marchiafava, *supra* note 17.

[29] A.P. MOLLER-MAERSK, *Annual Report 2017* (2018), https://investor.maersk.com/static-files/20a9e07d-0a49-4e36-a2c6-7d68a4dff918; Mhatre, *supra* note 7; Greenberg, *supra* note 9.

[30] *European Oil Facilities Hit by Cyber-Attacks*, BBC NEWS (Feb. 3, 2022), https://www.bbc.com/news/technology-60250956; *European Oil Terminals Hit by Cyberattack*, REUTERS (Feb. 3, 2022), https://www.reuters.com/business/energy/european-oil-terminals-hit-by-cyberattack-2022-02-03/; Marchiafava, *supra* note 17.

iv. COSCO Shipping (2018)

COSCO Shipping, a major Chinese container line, experienced a cyberattack on its network infrastructure in the Americas, affecting email systems and booking operations for days. The attack exposed the vulnerability of regional IT systems even within global conglomerates.[31]

v. GNSS spoofing in the Black Sea (2017)

Ships navigating the Black Sea reported misaligned GPS signals, later found to be the result of GNSS spoofing, a technique in which false location data is broadcast to deceive navigation systems. Such incidents demonstrate how cyber threats can compromise physical safety. These incidents, though diverse in execution, share common lessons: cybersecurity gaps, lack of preparedness, and insufficient regulatory harmonization.[32]

D. Legal and regulatory gaps

Despite growing awareness, maritime cybersecurity still suffers from fragmented regulation and uneven adoption of protective measures. There is no single, harmonized global legal standard governing maritime cybersecurity or cyber liability. Additionally, many cyberattacks go unreported, owing to reputational risk or legal ambiguity, which limits industry learning and hinders robust policy development. Insurance providers are also still grappling with how to define, underwrite, and indemnify against cyber risks in shipping.

As AI further complicates attribution and risk analysis, maritime cybersecurity must evolve not just through technical safeguards but also through legal standardization, information sharing, and cross-border enforcement cooperation.

The maritime industry stands at a complex intersection of digital innovation and security vulnerability. While the adoption of AI, automation, and smart logistics systems has revolutionized the sector, it has also magnified exposure to cyber threats. Understanding maritime cybersecurity means recognizing the layered nature of the risks, from software vulnerabilities and spoofed signals to deepfake identities and AI exploitation.

Real-world incidents and a growing body of literature make it evident that maritime security is no longer just about piracy and physical threats. The cyber domain is now equally, if not more, critical to ensuring the continuity, safety, and integrity of global maritime trade.

---

[31] *COSCO Shipping Lines Falls Victim to Cyber Attack*, OFFSHORE ENERGY (July 25, 2018), https://www.offshore-energy.biz/cosco-shipping-lines-falls-victim-to-cyber-attack/.

[32] Michael Jones, *Spoofing in the Black Sea: What Really Happened?*, GPS WORLD (Oct. 11, 2017), https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/.

III. LEGAL FRAMEWORKS FOR MARITIME CYBERSECURITY

As the maritime industry integrates digital systems ranging from ECDIS to automated port operations, it faces growing exposure to cyber threats. These risks demand more than technical safeguards; they require robust, multilayered legal frameworks to ensure accountability, preparedness, and international coordination. Cybersecurity in the maritime domain must therefore be examined through the lens of international law (IMO instruments and the United Nations Convention on the Law of the Sea), regional cooperation mechanisms, and national legislative models.

A. International legal frameworks

i. The role of the International Maritime Organization

The IMO is at the heart of global maritime governance. Recognizing the growing cyber threat landscape, the IMO adopted Resolution MSC.428(98),[33] which affirms that cyber risks should be addressed in ships' safety management systems (SMS) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.[34]

This resolution aligns cybersecurity with the ISM Code,[35] promoting operational resilience and continuity at sea. The IMO's Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) complement the ISM Code, urging shipping companies, port operators, and flag states to follow five functional elements of risk management: identify, protect, detect, respond, and recover.[36]

The International Ship and Port Facility Security (ISPS) Code, mandated by SOLAS Chapter XI-2, was originally developed to address physical threats to maritime security in the wake of the attacks of 11 September 2001.[37] However, its framework is now being interpreted to cover cybersecurity risks affecting the ship-port interface. Port facility security plans must now also consider threats arising from cyberattacks on the OT systems that control access, cargo, and berth scheduling.

[33] Res. MSC.428(98), *supra* note 12.
[34] Res. MSC.428(98), *supra* note 12, annex, para. 3.
[35] INTERNATIONAL MARITIME ORGANIZATION, Res. A.741(18), *International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code)* (Nov. 4, 1993), made mandatory under SOLAS ch. IX.
[36] MSC-FAL.1/Circ.3, *supra* note 23, annex, para. 3.5.
[37] International Ship and Port Facility Security (ISPS) Code, adopted by Conference Resolution 2 of the 2002 SOLAS Conference, IMO Doc. SOLAS/CONF.5/34 (Dec. 12, 2002), together with SOLAS ch. XI-2.

ii. The UNCLOS perspective

While UNCLOS does not directly address cybersecurity, it lays down foundational obligations that can encompass cyber governance. Article 94[38] imposes on flag states a duty to ensure that their ships conform to "generally accepted international regulations," a provision broad enough to include IMO cyber risk management standards. Moreover, UNCLOS Articles 211 and 218 govern pollution control and enforcement powers over foreign vessels. A cyberattack that compromises environmental safety (for example, by disabling ballast water treatment systems[39] or oil spill prevention mechanisms[40]) could fall within the jurisdictional powers granted under these articles. Under UNCLOS, states have binding obligations that can extend to cyber-induced marine hazards, especially in cases of transboundary harm such as a ransomware attack on a ship carrying dangerous goods. Article 192 establishes a general duty for states to protect and preserve the marine environment,[41] while Article 194(1) requires them to take all necessary measures to prevent, reduce, and control pollution of the marine environment from any source, which may include digitally mediated disruptions.[42] These duties have been interpreted broadly by international bodies. Notably, the International Tribunal for the Law of the Sea (ITLOS), in its advisory opinion of 21 May 2024, clarified that UNCLOS imposes a stringent due diligence standard on states, requiring legislative, administrative, and enforcement measures, as well as proactive cooperation and notification in cases of potential transboundary environmental harm.[43] Together, these provisions offer a legal and jurisdictional foundation for regulating and responding to cybersecurity threats in the maritime domain.

---

[38] United Nations Convention on the Law of the Sea art. 94(5), Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS].

[39] Ballast water treatment systems are onboard systems installed to manage ballast water, the water taken in by ships to maintain stability and trim during voyages. Before discharging this water, ships must treat it to remove harmful aquatic organisms and pathogens, as mandated by the International Convention for the Control and Management of Ships' Ballast Water and Sediments, Feb. 13, 2004 (BWM Convention).

[40] Modern ships use several systems to prevent accidental oil discharges. These include oil discharge monitoring equipment (ODME) to track oil content in water, oily-water separators (OWS) to filter bilge water, tank level sensors and overflow alarms to avoid spills, and secondary containment systems to catch leaks. While essential for environmental safety, these systems are increasingly digital and can be vulnerable to cyber threats.

[41] UNCLOS, *supra* note 38, art. 192; Jianping Guo, *The Developments of Marine Environmental Protection Obligation in Article 192 of UNCLOS and the Operational Impact on China's Marine Policy: A South China Sea Fisheries Perspective*, 120 MARINE POL'Y 104140 (2020), https://doi.org/10.1016/j.marpol.2020.104140.

[42] UNCLOS, *supra* note 38, art. 194(1); Cymie R. Payne, *Finding Light in Dark Places: Specific Obligations for Climate Change and Ocean Acidification Mitigation*, VERFASSUNGSBLOG (June 4, 2024), https://doi.org/10.59704/651d916278036d80.

[43] Request for an Advisory Opinion Submitted by the Commission of Small Island States on Climate Change and International Law, Case No. 31, Advisory Opinion (ITLOS May 21, 2024); *ITLOS Clarifies State Obligations Under UNCLOS in Relation to Climate Change*, SDG KNOWLEDGE HUB (IISD), https://sdg.iisd.org/news/itlos-clarifies-state-obligations-under-unclos-in-relation-to-climate-change/ (last visited Sept. 6, 2026).

B. Regional legal frameworks and cooperative mechanisms

i. The EU cybersecurity framework

The European Union integrates cybersecurity into maritime infrastructure through instruments such as the NIS 2 Directive,[44] which applies to essential and important entities in the transport sector, including ports. EU law mandates risk assessments, incident reporting, and supervisory controls. Additionally, the EU Maritime Transport Strategy encourages the adoption of cybersecurity requirements in port infrastructure upgrades and digital single-window systems. EU ports such as Antwerp-Bruges[45] and Rotterdam are already incorporating cyber resilience into smart port operations, using blockchain, IoT-enabled sensors,[46] and centralized vessel traffic services. These technological leaps have made compliance with cyber laws both urgent and complex, prompting regulators to align national rules with IMO frameworks.

ii. African maritime regions: the Djibouti Code and the Jeddah Amendment

The Djibouti Code of Conduct (2009)[47] and its Jeddah Amendment (2017)[48] are regional agreements facilitated by the IMO to combat piracy, armed robbery, and now broader maritime threats, including transnational organized crime in the maritime domain. These instruments emphasize inter-state cooperation, information sharing, training, and legal harmonization. While originally intended for kinetic threats such as piracy, the Jeddah Amendment's wider mandate has been read as capable of extending to cyber-enabled maritime crimes, such as hacking port logistics or manipulating AIS data. These agreements are critical for building regional capacity, especially in the Western Indian Ocean and the Gulf of Aden, where cybersecurity regulation is still developing.

iii. ASEAN and Pacific initiatives

Southeast Asian countries, particularly Singapore, are actively strengthening maritime cybersecurity frameworks in response to the vulnerabilities posed by chokepoints such as the Strait of Malacca. The Maritime and Port Authority of Singapore (MPA) has embedded cybersecurity requirements in its port and shipping regulation, giving effect to IMO instruments

[44] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union (NIS 2 Directive), 2022 O.J. (L 333) 80.
[45] PORT OF ANTWERP-BRUGES, *Smart Port*, https://www.portofantwerpbruges.com/en/our-port/port-future/smart-port (last visited Sept. 6, 2026).
[46] PORT OF ROTTERDAM, *Port of Rotterdam Puts Internet of Things Platform into Operation* (Jan. 31, 2019), https://www.portofrotterdam.com/en/news-and-press-releases/port-rotterdam-puts-internet-things-platform-operation.
[47] Code of Conduct Concerning the Repression of Piracy and Armed Robbery Against Ships in the Western Indian Ocean and the Gulf of Aden (Djibouti Code of Conduct), adopted Jan. 29, 2009.
[48] Jeddah Amendment to the Djibouti Code of Conduct, adopted Jan. 12, 2017, https://dcoc.org/about-us/jeddah-amendment/.

such as Resolution MSC.428(98) and MSC-FAL.1/Circ.3 through national measures, and has led international collaboration among port authorities on cyber resilience.[49] Singapore also launched a 24/7 Maritime Cybersecurity Operations Centre (MSOC), since expanded into the Maritime Cyber Assurance and Operations Centre (MCAOC), to provide real-time threat monitoring and coordination; by March 2025, sixteen companies had joined the MCAOC, and pooled monitoring is expected to save participants an estimated S$200,000 a year.[50] The MPA's broader initiatives include PACC-Net (the Port Authorities Chief Information Officer Cybersecurity Network), the MariOT testbed for OT cyberattack simulation and training, and the MaritimeSG Shipping CyberSafe Scorecard, developed with the Singapore Shipping Association to help maritime firms self-assess their cyber readiness against the NIST Cybersecurity Framework.[51] These measures are complemented by exercises such as Exercise CyberMaritime, which simulates coordinated ransomware attacks across ports to assess sectoral readiness.[52] Collectively, these initiatives make Singapore a regulatory and operational model for maritime cyber resilience in Southeast Asia.

C. National legal frameworks and enforcement

i. United States

The U.S. Coast Guard plays a regulatory role under the Maritime Transportation Security Act (MTSA). Section 70102(b)(1)(C) requires vulnerability assessments of vessels and facilities that identify weaknesses in, among other things, "security against cybersecurity risks" and "communications systems."[53] Section 70103(c)(3)(C) requires facility and vessel security plans to include provisions for "detecting, responding to, and recovering from cybersecurity risks."[54] The facility- and vessel-level security plans mandated by the Act therefore now explicitly include cyber risks. Ports also fall within the transportation systems sector that the Cybersecurity and Infrastructure Security Agency (CISA) treats as national critical infrastructure, requiring public-private coordination. Legal challenges in the United States stem from jurisdictional overlaps: state laws, federal regulations, and international conventions all

[49] MARITIME AND PORT AUTHORITY OF SINGAPORE, *MPA to Strengthen Collaboration on Cyber Resilience and Response at the 5th Port Authorities Roundtable* (Oct. 16, 2019), https://www.mpa.gov.sg/media-centre/details/mpa-to-strengthen-collaboration-on-cyber-resilience-and-response-at-the-5th-port-authorities-roundtable.

[50] MARITIME AND PORT AUTHORITY OF SINGAPORE, *Driving Growth and Innovation to Strengthen Maritime Competitiveness and Resilience* (Mar. 5, 2025), https://www.mpa.gov.sg/media-centre/details/driving-growth-and-innovation-to-strengthen-maritime-competitiveness-and-resilence.

[51] MARITIME AND PORT AUTHORITY OF SINGAPORE, *Collective Efforts to Strengthen Maritime Cybersecurity* (Apr. 16, 2024), https://www.mpa.gov.sg/media-centre/details/collective-efforts-to-strengthen-maritime-cybersecurity.

[52] MARITIME AND PORT AUTHORITY OF SINGAPORE, *Cybersecurity Initiatives* (undated).

[53] 46 U.S.C. § 70102(b)(1)(C).

[54] 46 U.S.C. § 70103(c)(3)(C)(v).

play a role. Courts have faced persistent challenges in applying traditional tort law principles to maritime cyber breaches, particularly regarding causation, foreseeability, and statutory limitations on liability. For example, the principle of reasonable foreseeability established in *The Wagon Mound (No. 1)*[55] limits liability to harm that could have been anticipated by a reasonable party. In cyber contexts, such foreseeability is often unclear, especially when vulnerabilities such as outdated ECDIS systems are exploited. If a breach occurs despite industry alerts or known risks, courts may find negligence based on a failure to meet evolving industry standards.[56] The U.S. Limitation of Liability Act further complicates recovery, allowing owners to cap damages unless the incident occurred with their privity or knowledge, as interpreted in cases such as *Parekh v. Argonautica Shipping Investments B.V.*[57] Similarly, in Canada's *Peracomo* case, the Supreme Court held that the shipowner retained the right to limit liability, but that his willful misconduct in cutting a submarine cable deprived him of insurance coverage.[58] Legal scholars argue that failing to patch known vulnerabilities could trigger liability under doctrines such as "no corrective precaution."[59] The lack of cyber-specific precedents in maritime tort law means that courts often fall back on analogies from traditional maritime negligence, creating uncertainty and legal grey zones in cyber-related claims.

ii. India's modernization scheme

India's Sagarmala Project, a flagship port modernization scheme, recognizes cyber resilience as essential to digital port transformation. The Directorate General of Shipping has required Indian-flag ships to incorporate cyber risk mitigation measures into their safety management systems in line with IMO Resolution MSC.428(98),[60] though no standalone, binding cyber code for the port sector exists yet. Indian ports, especially those operated under public-private partnerships, are encouraged to conduct periodic vulnerability assessments and adopt information security management systems (ISMS) in line with the ISO 27001 standard. However, a lack of uniform enforcement hinders full compliance.

---

[55] *Overseas Tankship (U.K.) Ltd. v. Morts Dock & Engineering Co. Ltd. (The Wagon Mound (No. 1))* [1961] AC 388 (PC).

[56] *Shipowners Financially Liable for a Cyber-Attack: Legal Expert*, SEATRADE MARITIME NEWS, https://www.seatrade-maritime.com/maritime-transportation/shipowners-financially-liable-for-a-cyber-attack-legal-expert (last visited Sept. 6, 2026).

[57] 46 U.S.C. § 30523 (formerly codified at 46 U.S.C. § 30505); *Parekh v. Argonautica Shipping Invs. B.V.*, 295 F. Supp. 3d 707 (E.D. La. 2018).

[58] *Peracomo Inc. v. Telus Communications Co.*, 2014 SCC 29, [2014] 1 S.C.R. 621 (Can.).

[59] Meiring de Villiers, *Distributed Denial of Service: Law, Technology & Policy* [2007] UNSWLRS 3, http://classic.austlii.edu.au/au/journals/UNSWLRS/2007/3.html.

[60] Res. MSC.428(98), *supra* note 12; DIRECTORATE GENERAL OF SHIPPING (India), *Implementation of Cyber-Security Risk Mitigation Measures Onboard Indian Flag Ships* (2017), as circulated in INDIAN REGISTER OF SHIPPING, Technical Circular No. 141/2017, https://www.irclass.org/technical-circulars/dg-shipping-circular-reg-implementation-of-cyber-security-risk-mitigation-measures-onboard-indian-flag-ships/.

D. Challenges in legal enforcement and liability

One of the major obstacles in maritime cyber law is legal ambiguity. Cyberattacks often involve cross-border actors, making attribution, jurisdiction, and enforcement highly complex. Traditional legal doctrines such as jurisdiction, causation, and foreseeability do not translate easily into the cyber domain.

Moreover, private actors such as third-party software vendors or digital navigation system providers create layers of liability that complicate fault attribution in cyber incidents. For example, if a malware-infected ECDIS system leads to a grounding, is the manufacturer liable, or the operator who failed to patch it? Cyber insurance in maritime law is still nascent. Most marine insurance policies lack explicit coverage for cyber incidents. Recent moves by Lloyd's and others to create separate cyber clauses are encouraging, but significant legal standardization is still required.[61]

E. Harmonization and capacity building

The need for harmonized legal instruments is critical. While IMO guidelines provide a global standard, their non-binding nature requires states to legislate and enforce them through national law. Classification societies and flag states must also be held accountable for cyber safety certifications. Capacity building is essential, particularly in developing regions. Programs funded by the IMO's International Maritime Security Trust Fund, along with the legal reform initiatives of the United Nations Office on Drugs and Crime (UNODC), help equip countries with training, legal toolkits, and forensic expertise to combat cyber incidents in ports and on vessels. Global cooperation will be vital in enabling legal interoperability. Future work may include drafting a model cybersecurity law for maritime nations, extending UNCLOS provisions through interpretive declarations, and integrating cybersecurity into port state control inspections. Cybersecurity in the maritime domain presents legal complexities far beyond conventional maritime risks. While the IMO and UNCLOS provide a structural backbone, enforcement gaps, jurisdictional fragmentation, and technical ambiguities hinder a coherent legal response. The integration of digital systems across ship and shore has made cyber threats a shared global concern, one requiring international collaboration, domestic legislation, and private-sector vigilance. The evolution of legal frameworks must be proactive, dynamic, and harmonized, ensuring that cyber resilience becomes as fundamental to maritime safety as life jackets and lifeboats.

[61] LLOYD'S MARKET ASSOCIATION, Bulletin LMA19-031-PD, *Property and Marine Cyber Clauses* (Nov. 13, 2019).

 [ISSN 2581-9453]

IV. Legal and technical challenges in maritime cybersecurity

The digitization of global shipping networks, the integration of IoT systems, and the adoption of AI-based tools have transformed the maritime sector into a technology-intensive domain. However, this digital evolution has outpaced legal, technical, and institutional safeguards, exposing ships, ports, and ocean infrastructure to serious cyber risks. Ransomware attacks on the maritime industry rose by around 60% in 2022 compared with 2020.[62] Legal ambiguity regarding jurisdiction, weak enforcement of international obligations, and vast disparities in cyber readiness across nations hinder the establishment of a secure global maritime ecosystem.

A. Jurisdictional challenges in maritime cybersecurity

Maritime cybercrimes, such as GPS spoofing, denial-of-service attacks on port systems, or malware attacks targeting navigation systems, often occur in jurisdictionally ambiguous zones such as the high seas or international port infrastructure. According to the *Lotus* case (1927),[63] international law permits states to extend their jurisdiction extraterritorially unless a prohibitive rule exists. This approach, however, becomes problematic in the maritime domain, where multiple states (the flag state, the coastal state, the port state, and the state of nationality of the victim) may have overlapping or conflicting jurisdictional claims.

The lack of harmonized rules for cyber incidents means that investigations, prosecutions, and reparations vary wildly. This fragmentation, as Marchiafava observes, has delayed the introduction of countermeasures against maritime cybercrime and poses enforcement difficulties.[64]

The maritime industry is undergoing a profound digital transformation. Ships are now equipped with integrated navigation systems, satellite communications, and remote monitoring sensors. Port infrastructure, too, is becoming increasingly automated through smart port initiatives. However, as these digital systems grow, so do cyber threats. From malware attacks on port logistics systems to GPS spoofing on the open seas, the attack surface has broadened. In 2017, the NotPetya malware attack on Maersk paralyzed seventeen of its port terminals and caused losses estimated at up to US$300 million, underscoring how cyber threats can disrupt the global economy.[65]

Yet international law, regulatory oversight, and technical standards have failed to evolve at the same pace. Jurisdictional ambiguities, the non-binding nature of IMO instruments, the lack of

[62] Department for Transport & Institution of Engineering and Technology, *supra* note 11.
[63] *S.S. Lotus (Fr. v. Turk.)*, Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18-19 (Sept. 7).
[64] Marchiafava, *supra* note 17.
[65] Marchiafava, *supra* note 17.

unified insurance frameworks, and asymmetrical cyber capabilities between nations pose significant barriers to global maritime cyber resilience.

Cyberattacks in the maritime domain often involve actors, assets, and consequences spanning multiple legal systems. Under UNCLOS, the flag state retains jurisdiction over ships on the high seas. However, in cyber incidents, port states, coastal states, or the states of nationality of the victims may all assert overlapping claims.

The Permanent Court of International Justice in the *Lotus* case (1927) observed that international law leaves states "a wide measure of discretion which is only limited in certain cases by prohibitive rules," so that "every State remains free to adopt the principles which it regards as best and most suitable," provided that it does "not overstep the limits which international law places upon its jurisdiction."[66] This means that states may exercise extraterritorial jurisdiction unless there is an explicit prohibition. Yet in cybercrime, this discretion results in legal chaos: differing national definitions of cyber offenses, incompatible data-sharing regimes, and political sensitivities over attribution.

The Budapest Convention on Cybercrime[67] offers a common framework, but several key maritime powers (for example, China, Russia, and India) are non-parties, limiting its effectiveness in transnational contexts. In such a vacuum, enforcement becomes slow or non-existent.

B. Non-binding nature of treaties and regulations

The IMO's Resolution MSC.428(98) calls on shipping companies to address cyber risks in their safety management systems under the ISM Code by January 2021. However, this resolution is non-binding, and its implementation depends entirely on whether flag states incorporate it into domestic legislation.[68] Similarly, MSC-FAL.1/Circ.3[69] and the guidelines issued by classification societies such as the Indian Register of Shipping and by national administrations such as the UK Department for Transport[70] provide valuable risk management recommendations, but these remain soft-law instruments. As a result, compliance varies drastically. Some flag states have developed robust audit frameworks, while others have failed

[66] *S.S. Lotus*, *supra* note 63, at 19.
[67] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (Budapest Convention).
[68] Res. MSC.428(98), *supra* note 12.
[69] INTERNATIONAL MARITIME ORGANIZATION, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3/Rev.2 (June 7, 2022), https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf.
[70] INDIAN REGISTER OF SHIPPING, *supra* note 14; DEPARTMENT FOR TRANSPORT & INSTITUTION OF ENGINEERING AND TECHNOLOGY, *supra* note 11.

to enforce even basic cybersecurity reporting standards. Some flag states have made significant strides in enforcing maritime cybersecurity standards, while others continue to fall short. For example, the Panama Maritime Authority requires the integration of cyber risk management into safety management systems, in line with IMO Resolution MSC.428(98), with compliance assessed during routine ISM audits and non-compliance exposing a vessel to the usual consequences of an ISM deficiency, including possible detention.[71] Similarly, registries such as Liberia and the Marshall Islands have aligned with the IMO mandate by requiring the inclusion of cyber risk in ship security and safety management arrangements, verified through audits following the first Document of Compliance verification after 1 January 2021.[72] In contrast, many flag-of-convenience states maintain only nominal or informal cyber reporting regimes and often lack enforcement capacity or incentive, enabling regulatory evasion. This concern has been noted in EU programming documents and in commentary highlighting weak oversight by some open registries and its implications for maritime safety and illicit activity.[73,74] This uneven enforcement underscores the urgent need for harmonized international standards and accountability across all flag states.

The ISPS Code,[75] originally designed for counterterrorism, does not clearly address cyber incidents, leading to regulatory overlap and enforcement ambiguity. Without a legally binding cybersecurity treaty akin to MARPOL (the International Convention for the Prevention of Pollution from Ships) or SOLAS (the International Convention for the Safety of Life at Sea), implementation and oversight remain voluntary.

C. Technical and operational issues

A critical vulnerability in maritime cybersecurity arises from the integration of outdated OT systems with modern IT frameworks aboard ships and within port infrastructure. Key onboard systems such as AIS, ECDIS,[76] GNSS, and RADAR[77] were not originally designed with cybersecurity in mind. These systems frequently operate without essential protections such as encryption, multi-factor authentication, or intrusion detection mechanisms, leaving them

[71] *2026 Maritime Cybersecurity Regulations: A Simplified Breakdown*, SHIP UNIVERSE (updated Jan. 23, 2026), https://www.shipuniverse.com/2025-maritime-cybersecurity-regulations-a-simplified-breakdown/.
[72] *2026 Maritime Cybersecurity Regulations*, *supra* note 71.
[73] EUROPEAN COMMISSION, Commission Implementing Decision of 25.4.2023 on the 2023 Annual Action Plan for the Global Threats Part of the Thematic Programme on Peace, Stability and Conflict Prevention (Apr. 25, 2023).
[74] Simon O. Williams, *Maritime Security: State Jurisdiction over PCASP*, THE MARITIME EXECUTIVE (Dec. 9, 2014), https://maritime-executive.com/article/Maritime-Security-State-Jurisdiction-Over-PCASP-2014-12-09.
[75] ISPS Code, *supra* note 37.
[76] Frank Akpan et al., *Cybersecurity Challenges in the Maritime Sector*, 2 NETWORK 123 (2022), https://doi.org/10.3390/network2010009.
[77] Aybars Oruc et al., *Perspectives on the Cybersecurity of the Integrated Navigation System*, 13 J. MARINE SCI. & ENG'G 1087 (2025), https://doi.org/10.3390/jmse13061087.

susceptible to cyber intrusion and manipulation. The risk is further amplified by common security lapses. Many vessels continue to rely on legacy software that remains unpatched, has no regular update mechanism, and is often incompatible with modern security protocols. Default or weak administrative credentials are frequently left unchanged, enabling unauthorized access with minimal effort. Additionally, the use of removable media such as USB drives, often inserted without proper scanning, introduces further avenues for malware infiltration. Maritime networks also rely heavily on satellite communication systems such as VSAT, which can be easily exploited if not adequately firewalled or isolated from mission-critical systems.

These vulnerabilities are not confined to ships alone. Smart ports, which depend on interconnected IoT ecosystems to manage automated cranes, track container movements, and facilitate customs operations, are exposed to similar cyber risks.[78] As Bronk and deWitte highlight,[79] much of the critical port infrastructure still relies on outdated firmware and control software, which cannot easily be replaced because of the high costs and the technical complexity of upgrading live systems; the shortage of cyber-skilled maritime personnel compounds the problem.[80] The attack on South Africa's Transnet in 2021[81] demonstrated the fragility of port operations in the face of cyber threats, as malware brought national logistics to a halt for several days, severely impacting trade flows.[82]

Despite this growing threat landscape, incident response in the maritime sector remains largely reactive. There is no globally mandated requirement for shipping companies or port authorities to conduct red-team exercises, establish security operations centers (SOCs), or implement real-time monitoring systems. As the article "Crucial Role of Shipping Agencies in Global Maritime Trade" emphasizes, many maritime operators lack even basic cybersecurity policies or formal crew training, leading to significant human-error vulnerabilities. In practice, phishing emails and social engineering attacks remain effective precisely because crew members are not trained to recognize or report them.[83]

---

[78] Kimberly Tam & Kevin Jones, *Maritime Cybersecurity Policy: The Scope and Impact of Evolving Technology on International Shipping*, 3 J. CYBER POL'Y 147 (2018), https://doi.org/10.1080/23738871.2018.1513053.

[79] Chris Bronk & Paula deWitte, *Maritime Cybersecurity: Meeting Threats to Globalization's Great Conveyor*, in CYBER SECURITY: CRITICAL INFRASTRUCTURE PROTECTION 241 (Martti Lehto & Pekka Neittaanmäki eds., 2022), https://doi.org/10.1007/978-3-030-91293-2_10.

[80] Júlia Grosschmid, *Addressing Maritime Workforce Cybersecurity Skills Development*, in MARITIME CYBERSECURITY 15 (Sanja Bauk ed., 2025), https://doi.org/10.1007/978-3-031-87290-7_2.

[81] Denys Reva, *Cyber Attacks Expose the Vulnerability of South Africa's Ports*, ISS TODAY (July 29, 2021), https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.

[82] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, *Case Study 17: Port of Durban, South Africa*, Resilient Maritime Logistics Guidebook, https://resilientmaritimelogistics.unctad.org/guidebook/case-study-17-port-durban-south-africa (last visited Sept. 6, 2026).

[83] *Crucial Role of Shipping Agencies in Global Maritime Trade*, *supra* note 1.

Compounding these issues is the lack of network segmentation on board vessels. Maritime networks often follow a flat architecture, meaning that once an attacker gains access through something as mundane as the entertainment system, they can potentially move laterally into navigation, engine, or safety control systems. Industry guidance therefore treats network segmentation and access control policies as core protective measures, yet their adoption across the world fleet remains uneven.[84] Without structural modernization, comprehensive training programs, and enforceable global standards, the maritime industry remains exposed to cyber threats that are growing in both frequency and sophistication.

D. Role of developed and developing nations

Cyber resilience in the maritime domain is unevenly distributed. Developed nations such as the United Kingdom, Norway, and Japan have national cybersecurity centers, conduct regular cyber drills, and publish detailed security codes of practice.[85,86] These countries also influence global standard-setting through their classification societies and flag registries. In contrast, many developing and underdeveloped countries, particularly those offering flags of convenience[87] (for example, Panama, Liberia, and the Marshall Islands), lack the regulatory or financial capacity to enforce cybersecurity standards. Ships under these flags are often not audited for cyber compliance, creating a global "weak link." Although initiatives such as the Djibouti Code of Conduct and its 2017 Jeddah Amendment aim to enhance maritime security in Africa and the Indian Ocean, cybersecurity is rarely their focus, and implementation is resource-constrained. Without targeted technology transfer, funding mechanisms, and training programs, the maritime sector in developing countries will remain vulnerable. Marchiafava notes that this asymmetry not only creates security risks but also undermines global trust in cross-border maritime cooperation.[88]

E. Maritime insurance and attribution of liability

Attribution of liability for maritime cyber incidents is a growing challenge. In the absence of explicit legal frameworks, blame often shifts among stakeholders: the shipowner may allege

[84] BIMCO et al., *supra* note 20 (recommending network segmentation and access control as core protective measures).
[85] DEPARTMENT FOR TRANSPORT & MARITIME AND COASTGUARD AGENCY, *Ports and Port Systems: Cyber Security Code of Practice* (Aug. 16, 2016, updated Jan. 27, 2020), https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice; DEPARTMENT FOR TRANSPORT & INSTITUTION OF ENGINEERING AND TECHNOLOGY, *supra* note 11.
[86] U.S. DEPARTMENT OF HOMELAND SECURITY, *DHS Partners with Japanese Counterparts to Strengthen Maritime Cybersecurity Cooperation* (Aug. 30, 2024), https://www.dhs.gov/archive/news/2024/08/30/dhs-partners-japanese-counterparts-strengthen-maritime-cybersecurity-cooperation.
[87] A flag of convenience refers to a situation in which a ship is registered in a country other than the one in which the ship's owner resides or holds citizenship; such a registry is often an "open registry".
[88] Marchiafava, *supra* note 17.

negligence by the software vendor, the port operator may deny responsibility for outdated control systems, and insurers may invoke exclusions for "acts of war" or "state-sponsored attacks."

The NotPetya attack on Maersk is instructive. Initially considered uninsurable under the "war exclusion" clause, it triggered industry-wide concern about coverage clarity.[89] Many marine insurance policies exclude cyber incidents unless they are explicitly covered under the Institute Cyber Clauses. Additionally, the lack of standardized definitions of "cyber event" or "cyber negligence" makes legal claims difficult to adjudicate. International law has yet to develop clear doctrines akin to strict liability, contributory negligence, or proximate cause for cyber scenarios, and courts struggle to apply traditional tort principles because of the lack of forensic attribution and the complex digital chains of causation. Without reform, victims of cyberattacks may find themselves without compensation, and perpetrators may evade accountability.

V. Conclusion and Recommendations

This paper has explored the cybersecurity landscape of the maritime industry through a cross-sectoral and interdisciplinary lens, examining industry practices, international regulatory efforts, technical standards, and real-world cyber incidents. High-profile cases such as the NotPetya ransomware attack on Maersk, the 2020 network breach at MSC, and the 2022 port terminal attacks in Europe underscore the potential for cyber threats to cause massive financial loss, supply chain disruption, and safety risks. The 2020 cyberattack on the IMO itself demonstrates that even regulatory authorities are not immune, further underscoring the urgency of comprehensive cyber resilience.

One of the central findings of this study is the inadequacy of current cybersecurity frameworks, which remain fragmented and largely voluntary. Unlike SOLAS and MARPOL, which provide binding global standards for safety and environmental protection, cybersecurity in the maritime domain lacks a universally enforceable legal instrument. While the IMO's Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) offer valuable direction, they fall short in terms of enforcement, leaving stakeholders with inconsistent implementation and oversight mechanisms. The result is a patchwork of national policies, port-level practices, and classification society requirements that do not uniformly secure the industry.

The convergence of IT and OT systems aboard vessels and within port infrastructure introduces additional complexity. Systems such as AIS, ECDIS, GNSS, RADAR, and VDR, though integral to maritime safety and navigation, can become points of cyber intrusion if not

[89] Marchiafava, *supra* note 17; Lloyd's Market Association, *supra* note 61.

adequately safeguarded. The integration of AI-driven systems used in autonomous navigation, predictive maintenance, and smart port operations has ushered in a new era of threat vectors. Advanced tactics such as data poisoning, algorithmic manipulation, and deepfake-enabled identity fraud are no longer hypothetical risks; they are plausible scenarios with potentially catastrophic consequences for maritime logistics and safety.

To address these challenges, a multi-pronged strategy is essential. First, there is an urgent need for regulatory harmonization. International bodies, including the IMO and the United Nations, should collaborate to develop a legally binding cybersecurity convention for the maritime domain, akin to SOLAS. Such a convention must incorporate provisions for incident reporting, minimum technical controls, information-sharing mechanisms, and international cooperation on enforcement and capacity building.

Second, classification societies and flag states must play a more proactive role in standard-setting and auditing. Initiatives such as the Indian Register of Shipping's cyber safety classification framework offer promising models that could be scaled globally. Regular cybersecurity audits and drills should be made mandatory, especially for high-risk operations involving automated or remote-controlled systems.

Third, technological resilience must be built into system architecture from the design stage. This includes implementing endpoint security, real-time anomaly detection, network segmentation, and secure-by-design principles for all maritime hardware and software systems. Given the growing role of AI, there is also a pressing need for AI-aware cybersecurity policies, particularly those that address adversarial machine learning and algorithmic integrity.

Fourth, capacity building and awareness remain critical. Many cyber incidents result not from technical failure but from human error: phishing attacks, weak credentials, and poor cyber hygiene. Crew training, stakeholder education, and routine cyber-awareness drills must become part of standard operating procedures. Investment in talent and workforce development will be as important as investment in firewalls and software.

Finally, global cooperation and information sharing are imperative. Cyberattacks do not respect jurisdictional boundaries, and a successful defense requires coordinated international response mechanisms. Maritime Information Sharing and Analysis Centers (ISACs), regional forums, and joint exercises among naval, commercial, and port authorities should be expanded and institutionalized.

As the maritime industry sails deeper into the digital age, cybersecurity can no longer be treated as an auxiliary concern. It must be embedded in the core of operational planning, legal

 [ISSN 2581-9453]

frameworks, and technological innovation. Only through an integrated, anticipatory, and collaborative approach can the global maritime community build a resilient, secure, and future-ready ecosystem, one that ensures the continuity of international trade, the protection of lives and assets, and the stability of the maritime commons. Cyber threats in the maritime domain represent a clear and present danger to international trade, security, and economic stability. A coordinated global legal and technical response is urgently needed, one that reflects both the complexity of the cyber domain and the diversity of maritime stakeholders.

*****

 [ISSN 2581-9453]