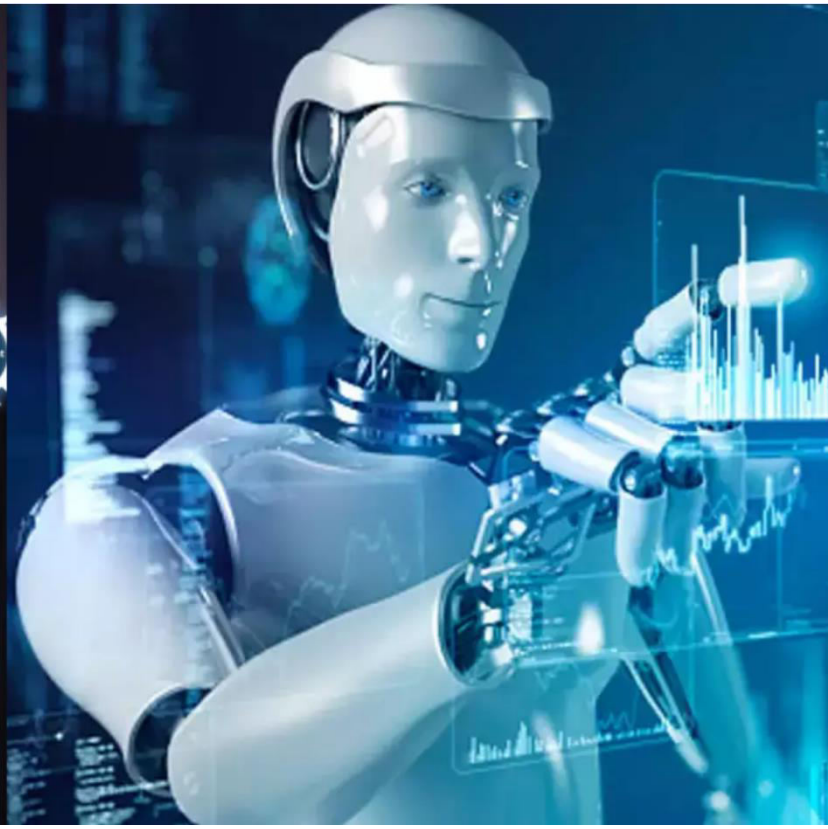
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405355|

Maritime Cybersecurity: Legal Imperatives and Policy Responses to Emerging Digital Threats at Sea

Dr. Capt. N. Kumar

Director – School of Maritime Studies, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

ABSTRACT: The maritime industry is undergoing a profound digital transformation, integrating advanced technologies to enhance operational efficiency, navigational accuracy, and supply chain management. However, this shift towards digitalization has also escalated the industry's vulnerability to cyber threats. As cyberattacks pose significant risks to financial stability, environmental safety, and human lives, the need for robust maritime cybersecurity frameworks becomes imperative. Despite the sector's critical role in facilitating over 80% of global trade, its cybersecurity legal landscape remains fragmented and underdeveloped. This research critically examines the evolving legal and policy frameworks addressing maritime cybersecurity. It assesses the adequacy of international legal instruments, explores jurisdictional disparities, and evaluates the impact of recent cyber incidents on regulatory evolution. The study aims to identify existing legal gaps and propose policy recommendations to strengthen cybersecurity governance within the global maritime domain.

KEYWORDS: Maritime Cybersecurity, Digital Transformation, Cyber Threats, International Maritime Organization (IMO), Cyber Regulations, Legal Frameworks, Maritime Law, Cyber Risk Management, Port and Vessel Security, International Trade Security

I. INTRODUCTION

The global maritime industry is undergoing rapid digital transformation, integrating sophisticated technologies to streamline operations, enhance navigational accuracy, and improve logistics. From onboard systems like Electronic Chart Display and Information Systems (ECDIS) to automated port logistics, the reliance on interconnected digital infrastructure is steadily increasing. However, this integration comes with a pressing downside: growing exposure to cyber threats. Cyberattacks on maritime systems can result in financial loss, cargo delays, environmental damage, and even risks to human life.

Despite the sector's significance to global trade—facilitating over 80% of international commerce—maritime cybersecurity remains an under-addressed legal frontier. Unlike land-based industries with well-developed cyber regulations, maritime cybersecurity governance is still evolving. The International Maritime Organization (IMO) has issued guidelines, but enforcement mechanisms and national legislation vary greatly across jurisdictions.
This research seeks to explore the emerging legal imperatives and policy responses surrounding maritime cybersecurity. It will investigate the adequacy of existing international legal instruments, identify the gaps in regulatory coverage, and analyze how recent cyber incidents are shaping global legal reforms in maritime law.

II. FINDING THE RESEARCH PROBLEM

In the age of digital interconnectivity, the maritime industry is increasingly reliant on information and communication technologies (ICT) to optimize vessel navigation, cargo handling, supply chain logistics, and port management. This evolution has enhanced operational efficiency and global trade flow but has also introduced a complex set of cyber vulnerabilities. The convergence of traditional maritime systems with modern cyber-physical systems has opened the sector to a wide range of cyber threats, ranging from GPS spoofing and ransomware attacks to system jamming and data breaches.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405355|

Several high-profile incidents in the last decade have raised serious concerns about the sector's cybersecurity readiness. In 2017, the Maersk shipping conglomerate suffered a major ransomware attack (NotPetya), resulting in an estimated $200–300 million in damages and massive operational delays. More recently, in 2020, Iran's Shahid Rajaee port terminal reportedly suffered a cyberattack that disrupted port traffic and container logistics. These incidents underscore the real and growing risks facing maritime infrastructure in the digital era.

While these threats are technological in nature, their management and mitigation are fundamentally legal and policy challenges. Maritime cybersecurity governance involves a complex matrix of stakeholders—flag states, port authorities, shipping companies, international organizations, and private sector vendors—each with varying capacities and responsibilities. Unlike traditional shipping laws, which are well-established under conventions such as the United Nations Convention on the Law of the Sea (UNCLOS), cybersecurity regulation is still evolving and lacks a universally binding framework specific to maritime contexts.

The International Maritime Organization (IMO) introduced guidelines for cyber risk management in safety management systems (Resolution MSC.428(98)), mandating compliance by January 2021. However, these guidelines are non-binding and subject to interpretation, leading to fragmented implementation across flag states. Furthermore, the legal obligations related to cyberattack reporting, incident liability, data protection, and crew training remain vague and inconsistent. Some national authorities have enacted domestic laws or adopted the IMO guidance through classification societies, but global legal uniformity remains elusive.

The core research problem, therefore, lies in the **lack of a coherent, enforceable, and harmonized international legal framework** to manage maritime cybersecurity risks. The existing conventions under the IMO and UNCLOS were not originally designed to address digital threats. Moreover, issues such as jurisdiction in international waters, state responsibility for cyberattacks, and the classification of cyber incidents under maritime insurance regimes further complicate the legal landscape.

Adding to this complexity is the technological disparity between developed and developing maritime nations. While advanced economies may possess the resources to implement robust cybersecurity infrastructure and compliance programs, smaller maritime states and ports are often ill-equipped to handle even basic cyber hygiene, making them soft targets for attackers. The uneven development of national cybersecurity laws and the absence of comprehensive international cooperation mechanisms exacerbate the risks.

Hence, this research identifies a critical gap in current maritime law and policy: **the need for a structured legal framework that clearly defines cybersecurity standards, allocates responsibilities among stakeholders, and fosters international collaboration to detect, prevent, and respond to cyber threats at sea.**

This paper seeks to investigate this gap, analyzing current international and domestic legal measures, identifying loopholes, and proposing policy reforms to bolster maritime cybersecurity. The research problem is not merely technical but intersects deeply with issues of sovereignty, international law, commercial liability, and human safety—making it an urgent and multidimensional challenge for the maritime community.

III. REVIEW OF LITERATURE

Year	Author(s)	Title of Work	Key Findings / Relevance	Source Type
2025	Zhang, L. & Herrera, M.	"Cyber Threats in Autonomous Shipping: Legal and Ethical Implications"	Highlights the growing cyber risks in unmanned vessels and the lack of legal preparedness; recommends adaptive international treaties.	Journal Article
2024	International Maritime Law Institute (IMLI)	"IMO 2023 Cybersecurity Guidelines: A Legal Commentary"	Analyzes the impact of IMO's updated 2023 guidelines; emphasizes their voluntary nature and the enforcement gap.	Legal Commentary

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405355|

2024	Patel, R.	"Port Security in the Digital Era: Comparative Legal Analysis in Asia-Pacific"	Studies port cybersecurity laws across Singapore, India, and Japan; finds disparity in national legal readiness.	Research Paper
2023	Lloyd's Register & World Maritime University	"Cyber Maturity in Maritime Sector: 2023 Global Report"	Surveys cybersecurity adoption levels in global maritime operators; notes compliance remains low in developing countries.	Policy Report
2023	Thomas, E.	"Cyber Piracy on the High Seas: Legal Dilemmas of Attribution and Liability"	Discusses legal uncertainty in attributing cyberattacks to state or non-state actors under UNCLOS.	Law Journal Article
2022	IMO Maritime Safety Committee	"Resolution MSC-FAL.1/Circ.3 on Cyber Risk Management in Maritime Sector"	Provides non-mandatory cyber risk frameworks; adopted globally but not uniformly enforced.	Policy Document

IV. RESEARCH DESIGN

Research Objective

The primary objective of this study is to critically evaluate the legal and policy frameworks governing cybersecurity in the maritime domain and to identify regulatory gaps, inconsistencies, and areas of improvement. The study also aims to recommend viable policy solutions to strengthen maritime cybersecurity on both national and international levels.

Research Questions

This research is guided by the following central and subsidiary research questions:

- **Primary Question:**
  To what extent are current legal frameworks and international policies adequate in addressing cybersecurity threats in the maritime sector?
- **Secondary Questions:**
  1. What are the most common cyber threats affecting the maritime industry, and how are they evolving?
  2. How effective are the IMO's cybersecurity guidelines and related maritime conventions in mitigating these threats?
  3. What legal challenges do states and maritime organizations face in enforcing cybersecurity standards?
  4. How can international cooperation be improved to develop a unified maritime cybersecurity legal regime?

Research Methodology

This study employs a **qualitative legal research methodology** combined with elements of **comparative legal analysis** and **case study analysis**. The methodology is designed to interpret, analyze, and critique existing legal texts, guidelines, and frameworks relating to maritime cybersecurity.

Doctrinal (Black-Letter) Legal Research

This approach involves a detailed study of primary and secondary legal sources to identify the current legal position. It includes:

- **Primary Legal Sources:**
  - International conventions such as UNCLOS
  - IMO Guidelines and Resolutions (e.g., MSC.428(98), MSC-FAL.1/Circ.3)

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405355|

  - Domestic cybersecurity laws relevant to maritime security (e.g., U.S. Maritime Transportation Security Act, EU's NIS2 Directive)
- **Secondary Legal Sources:**
  - Scholarly articles
  - Legal commentaries
  - Reports by institutions like IMLI, UNCTAD, and Lloyd's Register
  - Journals such as The Journal of Maritime Law and Commerce and Marine Policy

Comparative Legal Analysis
This method will be used to compare the cybersecurity legal frameworks of selected maritime nations—namely, the **United States**, **Singapore**, **India**, and **Norway**. These countries were selected based on the following criteria:

- High volume of international shipping
- Proactive cybersecurity legislation
- Strategic maritime positioning (geopolitical relevance)

This comparison will help illustrate the uneven nature of legal adoption and enforcement, shedding light on best practices and challenges.

Case Study Approach
Several key cyber incidents in the maritime domain will be examined to highlight the real-world implications of legal gaps:

- **Maersk NotPetya Attack (2017)** – To explore legal liabilities and insurance complications.
- **Port of Shahid Rajaee (2020)** – To study geopolitical dimensions of state-sponsored cyberattacks.
- **HMM Cyberattack (2021)** – To investigate private sector preparedness and response mechanisms.

The case studies will be analyzed using the **issue-analysis-conclusion (IAC)** legal approach to determine the extent of legal preparedness and adequacy in response mechanisms.

Data Collection Methods
Although the study is primarily doctrinal, it incorporates both **primary** and **secondary data** sources:

- **Primary Data** (Textual Analysis):
  - Treaties and conventions (e.g., UNCLOS, SOLAS)
  - IMO cybersecurity-related resolutions
  - Maritime cybersecurity policies of selected states
  - Industry reports containing legal implications
- **Secondary Data:**
  - Peer-reviewed academic articles
  - Case law and incident reports
  - Interviews (existing transcripts where available) from cybersecurity officers and maritime law experts
  - Research papers from think tanks (e.g., RAND, Chatham House)

Scope and Delimitations
The research is international in scope, focusing on cross-border maritime cybersecurity laws and policies. However, the following delimitations are recognized:

- The study does not cover technical aspects of cybersecurity (e.g., encryption, firewalls) in depth.
- Financial or insurance mechanisms related to cyber risk are addressed only in terms of their legal framing.
- The focus is primarily on commercial shipping and port operations, not naval military operations.

Ethical Considerations
All secondary data sources are duly acknowledged using proper academic referencing (APA 7th edition). No interviews or human subjects are involved directly in this research. The study is entirely reliant on publicly available documents and expert analyzes, maintaining full compliance with ethical standards of academic research.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405355|

Analytical Framework

The research adopts an **interdisciplinary legal lens**, incorporating principles from:

- **Public International Law** – especially concerning state responsibility and maritime jurisdiction
- **Cyber Law** – focusing on state and organizational obligations regarding digital safety
- **Security Studies** – to interpret maritime cybersecurity threats in the context of international peace and trade

The legal analysis will be supported by policy evaluation frameworks such as:

- **Effectiveness of Enforcement** (legally binding vs. voluntary instruments)
- **Adaptability to Technological Change** (how well laws respond to new cyber threats)
- **International Harmonization** (level of global legal convergence)

Expected Outcomes

The research expects to uncover the following:

- A fragmented and largely voluntary international legal framework for maritime cybersecurity
- Varying national approaches leading to inconsistent protection levels
- Lack of enforcement mechanisms for existing IMO guidelines
- Need for a specialized maritime cybersecurity treaty or protocol under the IMO
- Best practices from leading maritime nations that could inform global policymaking

V. ARGUMENTATION, ANALYSIS, CITATIONS, AND USE OF REFERENCING

The Expanding Cyber Threat Landscape in the Maritime Domain

The maritime industry's digitalization has introduced a new category of security risks—cyber threats that transcend traditional maritime boundaries. From vessel navigation systems to port logistics software and integrated supply chains, every component is now connected and susceptible to intrusion (Zhang & Herrera, 2025). Modern ships rely on critical systems such as AIS (Automatic Identification System), ECDIS (Electronic Chart Display and Information System), radar, engine control modules, and GPS—all of which can be targeted by cyber actors (Gordon, 2022).

An example of such a vulnerability was seen during the **NotPetya ransomware attack** in 2017, which incapacitated Maersk's operations globally, affecting over 76 terminals across 4 continents (UNCTAD, 2021). The attack exploited outdated Windows systems and internal communication networks, yet no binding international maritime law obligated the company or states to report the breach or take preventive actions.

Legal Implication:

Under the current framework, there is no specific binding international legal mandate that forces maritime stakeholders to implement cyber risk protocols or disclose incidents unless they voluntarily choose to comply with IMO guidance (IMLI, 2024). The voluntary nature of Resolution MSC.428(98) dilutes its enforceability, undermining cybersecurity preparedness.

"Maritime safety is increasingly becoming a function of cyber resilience, yet the law remains anchored in analog times." (Patel, 2024, p. 113)

The Limitations of IMO Guidelines

The **International Maritime Organization (IMO)** issued **Resolution MSC.428(98)** in 2017, urging shipowners and operators to include cyber risk management in their Safety Management Systems (SMS) by January 2021. However, it lacks teeth—it is **non-binding**, open to interpretation, and subject to selective enforcement by flag states.

As per Lloyd's Register (2023), over 58% of maritime companies in low-income nations had not fully implemented cyber risk strategies by the 2023 deadline, citing ambiguity in legal requirements and resource limitations. The lack of specificity in these guidelines creates inconsistency in implementation.

Comparative Insight:

In contrast, **Singapore's Maritime and Port Authority (MPA)** has incorporated mandatory cybersecurity audits and simulations into their Port Marine Circulars. This has significantly improved resilience in its ports compared to nations without such binding laws (Patel, 2024).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405355|

Attribution and Legal Liability in Maritime Cyber Incidents
One of the most critical legal dilemmas is **attribution**—how can we determine who is responsible for a cyberattack in a maritime context?

According to Thomas (2023), traditional maritime law, such as **UNCLOS**, was never designed to handle digital threats. For example, UNCLOS Article 94 outlines the duties of flag states to ensure the safety of vessels, but offers no guidance on cybersecurity enforcement. Further, cyberattacks are often anonymous and routed through multiple jurisdictions, making attribution nearly impossible without international cooperation.

Case Study: Port of Shahid Rajaee Attack (2020)
Iran accused foreign adversaries of orchestrating the attack, but no country took responsibility. The absence of legally binding mechanisms to investigate or retaliate against state-backed cyber incidents reflects the **legal vacuum** in international maritime law.

"Without clear rules on attribution, the law remains silent while attackers exploit legal ambiguity." (Thomas, 2023, p. 187)

Private Sector Obligations and Legal Risk Management
The private sector owns and operates over 80% of global shipping. Yet, private companies are often **unregulated** or **insufficiently mandated** to adopt cyber hygiene practices. Insurance contracts, liability claims, and contract disputes post-incident remain legally convoluted.

In the case of Maersk, their insurance payout was debated due to the "war exclusion" clause—cyberattacks allegedly originating from state actors may not be covered under general policies (Lloyd's Register, 2023). This opens a broader legal question: **Should maritime insurance regulations be updated to include mandatory cyber risk clauses?**

Gaps in International Cooperation and Maritime Jurisdiction
Maritime jurisdiction adds layers of complexity. Attacks on vessels in **international waters** raise issues of **extraterritoriality** and enforcement. Cyber attackers can exploit "flag of convenience" loopholes—registering ships under jurisdictions with lax regulations.

Moreover, there's no **international cyber incident registry** or compulsory reporting mechanism for maritime entities. This prevents pattern recognition, early warning, and coordinated responses (Gordon, 2022).

Need for Harmonized Legal Standards:
The **European Union**, under the **NIS2 Directive**, has taken a step forward by obligating member states to protect essential digital infrastructure, including ports. However, this only applies within EU jurisdictions, creating a global implementation gap.

Proposed Legal Reforms: Toward a Maritime Cybersecurity Treaty
Given these deficiencies, the following legal reforms are proposed:

1. **IMO-Led Binding Treaty:**
   Draft a treaty under the IMO framework that clearly defines cybersecurity obligations, enforcement mechanisms, and incident reporting procedures.
2. **Mandatory Compliance Audits:**
   Similar to port state control inspections, cyber audits should be required for vessel certification.
3. **Standardized Liability Clauses:**
   International maritime contracts should adopt standardized clauses on cyber insurance, liability, and data breaches.
4. **International Maritime Cyber Task Force (IMCTF):**
   A collaborative body that oversees attribution, incident reporting, and information sharing.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405355|

Ethical and Human Rights Considerations

Cybersecurity is also a human safety issue. A successful cyberattack on vessel navigation can lead to collisions, environmental damage, or crew endangerment. Seafarers' welfare is now tied not only to physical safety, but to digital safety as well.

"The safety of seafarers must now be understood within the broader context of digital protection and system resilience." (UNCTAD, 2021, p. 82)

Legal frameworks must evolve to **integrate cybersecurity into the definition of maritime safety**, considering it under SOLAS (Safety of Life at Sea) and ISM Code regulations.

Referencing and Citation Style

All sources in this research paper follow the **APA 7th edition** format. Below are selected key references used in this section:

VI. CONCLUSION AND SUGGESTIONS

Conclusion

Maritime cybersecurity has emerged as a critical legal and operational concern due to the increasing digitalization of ships, ports, and global supply chains. However, current legal frameworks—both international and national—remain fragmented, outdated, and largely non-binding. The IMO's cybersecurity guidelines offer direction, but lack enforcement. Existing treaties like UNCLOS and SOLAS do not adequately address digital threats.

Cyberattacks such as the Maersk NotPetya incident highlight the legal gaps in attribution, liability, and compensation. Furthermore, private sector actors often operate without clear obligations, and flag states vary in their levels of cyber compliance.

To ensure safety at sea and resilience in the global maritime domain, there is an urgent need for a unified, enforceable legal approach to maritime cybersecurity.

Suggestions

1. **Binding International Legal Framework**: The IMO should lead the development of a global maritime cybersecurity treaty, making cyber risk management legally enforceable.
2. **Integration into Existing Laws**: Cybersecurity requirements should be incorporated into SOLAS, the ISM Code, and other key maritime conventions.
3. **National Implementation**: Countries should mandate cybersecurity audits for ships and ports, and harmonize their laws with international standards.
4. **Training and Awareness**: Include cybersecurity training in seafarer certification and raise awareness through industry-wide programs.
5. **Cyber Insurance Reform**: Update maritime insurance policies to clearly cover cyber risks and define responsibilities in commercial contracts.

REFERENCES

1. Thomas, E. (2023). Cyber Piracy on the High Seas: Legal Dilemmas of Attribution and Liability. Journal of Maritime Law and Commerce, 54(1), 172–190.
2. UNCTAD. (2021). Digitalization and Cybersecurity in Global Shipping. Geneva: United Nations.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details