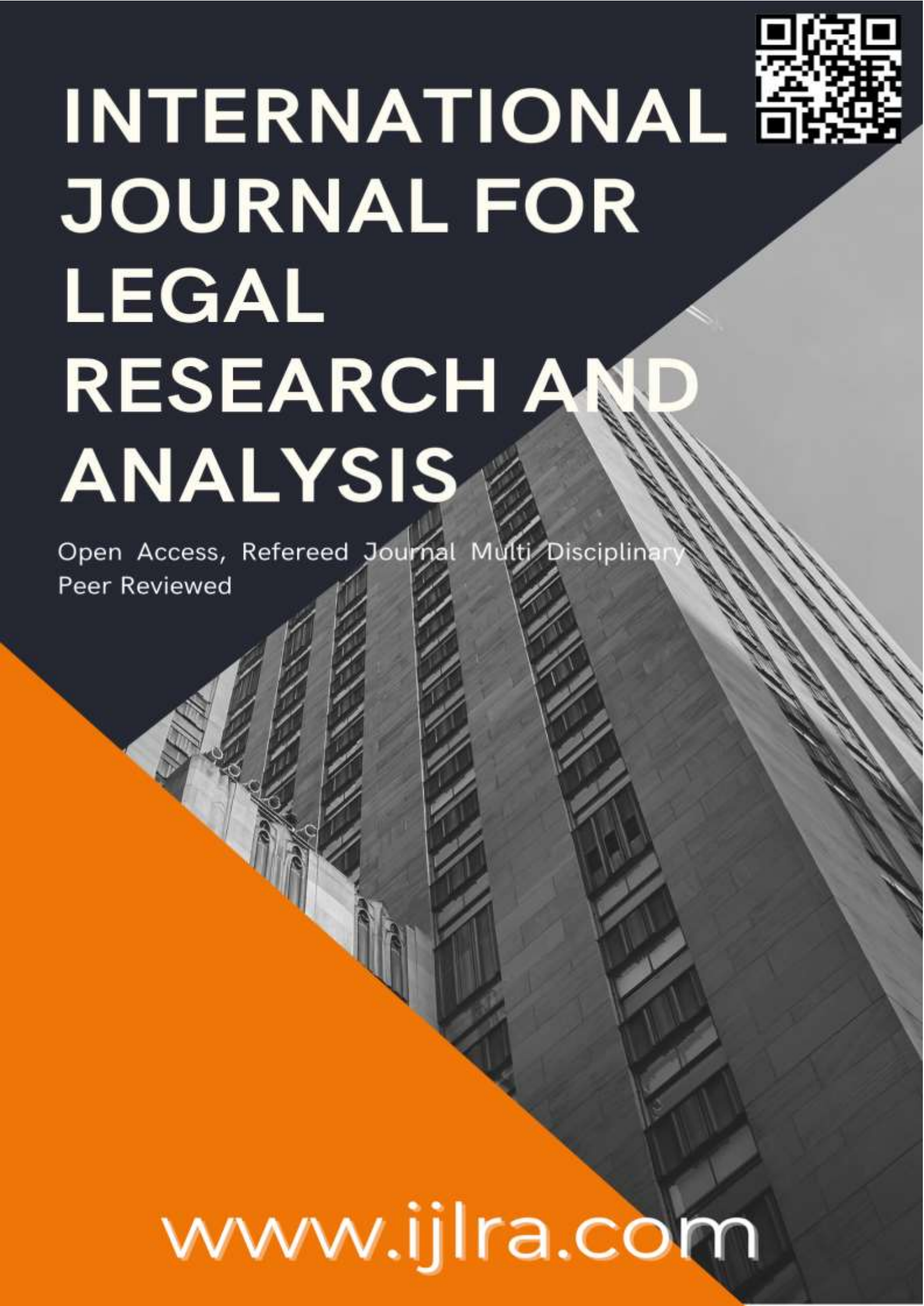
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

PHISHING VESSELS AND COMPROMISING PORTS - AN ANALYSIS OF CYBERCRIMINAL ACTIVITIES TARGETING THE MARITIME SECTOR

AUTHORED BY - AZIMATHUL MARSHIYA M,
JEYAMURUGAN S & NANDHINI PRIYA S P

ABSTRACT

The maritime industry, once dominated by physical risks, is now increasingly vulnerable to cyber threats due to rapid digitalization. This paper examines the growing threat of cybercrime in the maritime sector, specifically through phishing attacks and systemic intrusions targeting vessels and port infrastructure. As Information Technology and Operational Technology systems become more integrated, poor segmentation between them enables hackers to disrupt navigation, cargo operations, and even ship control systems. Ports are highly susceptible to cyber intrusions have resulted in smuggling, cargo rerouting, and operational paralysis.

Beyond technological vulnerabilities, human factors significantly contribute to cyber risks. Phishing attacks and social engineering tactics exploit seafarers and staff, leading to unintended data breaches and malware installations. Case studies such as the 2017 Maersk ransomware attack and the cyber breach at COSCO Shipping highlight the real-world impact, including global shipping disruptions and financial losses. Instances of GPS spoofing in strategic maritime zones further illustrate the potential for geopolitical and navigational crises. Despite international efforts, such as the International Maritime Organization's cybersecurity mandate and the EU's Network and Information Systems Directive, major gaps remain. Many vessels still rely on outdated systems, cybersecurity training is insufficient, and global coordination is fragmented.

This study argues for a holistic and people centered approach to maritime cybersecurity. It recommends the implementation of secure digital architecture, mandatory training programs, awareness campaigns on phishing and social engineering, and resilient navigation backups like eLoran. Emphasizing proactive rather than reactive strategies, the paper advocates for robust collaboration between shipping companies, port authorities, regulatory bodies, and cybersecurity experts. As maritime trade becomes increasingly reliant on digital networks,

ISSN: 2582-6433

cybersecurity must be viewed as an essential pillar of maritime safety, economic resilience, and the protection of global trade routes.

Keywords:
Cybersecurity, Maritime Navigation, GPS Spoofing, AIS Tampering, IMO Guidelines, Maritime Digital Risk. Port Infrastructure Vulnerability,

I. INTRODUCTION

Over 90% of global trade by volume is made possible by modern maritime infrastructure, which serves as the circulatory system of the globalized economy. Shipping's dependence on cyberspace creates new avenues for criminal exploitation as digital technologies such as satellite navigation, AI-driven logistics, automated port operations, and integrated logistics management become more and more integrated into the industry. Phishing is one of the most prevalent and sneaky of these threats, with hackers using false communications to compromise shipping companies, alter cargo manifests, and take control of critical operational data[1]. As a result of the marine industry's shift to smart technology, it has become a prime target for sophisticated attacks. Examples of these attacks include GPS spoofing that jeopardizes vessel navigation and ransomware lockouts of vital port infrastructure.

With 13 major ports and more than 200 minor ports, India's maritime sector is the focal point of this danger[2]. Strong cybersecurity measures and legal protections have not kept pace with the nation's fast digitization of port operations and shipping logistics. Cybercriminals can now operate with relative impunity thanks to a combination of issues, such as antiquated IT systems, ad hoc cyber risk management, and a lack of legal understanding among marine stakeholders. The problem is made worse by the lack of marine cybercrime laws tailored to India, which forces port authorities and local shipping businesses to rely on general information technology rules that are unable to handle the subtleties of maritime cyberthreats.

Though unevenly, the legal and regulatory environment is changing globally. A growing awareness of the need for baseline cybersecurity standards is shown in the International

[1] Dualog, Stay Ahead of Emerging Email Threats at Sea (Apr. 7, 2025), available at https://dualog.com/stay-ahead-of-emerging-email-threats-at-sea/ (last accessed Aug. 1, 2025).
[2] International Maritime Organization, Guidelines on Maritime Cyber Risk Management, IMO MSC-FAL.1/Circ.3/Rev.2, 2021,

ISSN: 2582-6433

Maritime Organization [3], which requires shipping companies to include cyber risk management into their safety management systems. Although neither was created to handle the particular jurisdictional and evidentiary difficulties presented by maritime cybercrime, international agreements like the United Nations Convention on the Law of the Sea (UNCLOS) and the Budapest Convention on Cybercrime offer fundamental guidelines for state collaboration and criminal prosecution[4]. Amidst this legal void, many nations and regional organizations most notably the European Union, under its Network and Information Systems (NIS) Directive have initiated the imposition of mandatory cybersecurity requirements on operators of vital marine infrastructure[5].

The legal ramifications of cybercrime directed at the maritime industry are examined in this essay, with particular attention on phishing-based assaults that jeopardize both ships and port infrastructure. It examines whether current international frameworks are adequate to combat cyber-enabled maritime crime and critically evaluates the regulatory vacuum in India by comparing it to emerging jurisprudential developments in other maritime states. By doing this, the research draws attention to the pressing need for unified laws, international enforcement strategies, and capacity-building programs in order to protect one of the most important and vulnerable economic infrastructures in the world.

II. THE ANATOMY OF MARITIME CYBERCRIME

Due to the shift to digital technologies, the marine industry is now subject to a wide range of constantly changing cybercrime activities, each with its own unique tactics and potential legal ramifications. Cyberattacks against shipping companies can take many different forms, each specifically designed to take advantage of the special weaknesses of marine infrastructure, from the boardroom to the bridge. The structure of these crimes exposes the systemic dangers in maritime cybersecurity governance as well as the inventiveness of the attackers[6].

Social engineering and phishing*:* The human factor continues to be the most vulnerable entry

[3] International Maritime Organization [IMO], Maritime Cyber Risk Management in Safety Management Systems, IMO Res. MSC.428(98), Annex 10 (adopted June 16, 2017), available at https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428%2898%29.pdf

[4] D. Melnyk, Cybersecurity in Maritime Transport: An International Perspective on Legal Regulation, Lex Portus, vol. 11, no. 1, pp. 11–13 (2025),

[5] DNV, Maritime Cyber Security Regulations, available at https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/regulations/ (last accessed Aug. 4, 2025).

[6] International Maritime Organization, Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.2, 2021,

ISSN: 2582-6433

point for cyberattacks. Phishing emails, which are deliberately designed to look like authentic correspondence, are frequently sent to workers of shipping companies, port authorities, and even crew members. These emails frequently act as the first point of entry, making it possible to steal credentials or secretly install malware on business networks and operational technology systems[7]. Although not solely a maritime attack, the 2017 NotPetya incident exemplified the ripple effects of such intrusions: malware spread through compromised accounting software quickly encrypted IT systems throughout Maersk's international operations, paralyzing terminals, stranding ships, and causing losses of over $300 million[8]. The disastrous operational and financial outcomes that occur when cybersecurity readiness falls behind digital transformation were highlighted in this episode.

Ransomware: Attacks using ransomware have increased in frequency, affecting both IT and operational technology (OT) systems in ports and on board ships. Attackers take maritime operations hostage by encrypting vital data, such as cargo manifests and navigation logs, and then demanding cash to unlock it. Given the international nature of shipping and the jurisdictional difficulties present in cybercrime cases, such attacks not only cause supply chain disruptions but also bring up difficult liability issues[9]. The legal framework for dealing with ransomware in the maritime environment is still in its infancy, especially in countries like India. As a result, victims are frequently forced to rely on general cybercrime laws that do not take into consideration the unique hazards associated with the industry[10].

GPS Spoofing and Hijacking: For marine safety, a vessel's navigation equipment must be reliable. The capacity to spoof or jam GPS signals has been shown by state-sponsored actors and cybercriminals, which can lead to erroneous navigational data and confuse ships' Electronic Chart Display and Information Systems (ECDIS). Such tampering may cause unapproved diversions, collisions, or groundings, which might have catastrophic effects on the environment and security. The legal framework that regulates these activities is also disjointed: although the IMO has published guidelines for managing cyber risks, there isn't a legally

[7] Dualog, Stay Ahead of Emerging Email Threats at Sea (Apr. 7, 2025), https://dualog.com/stay-ahead-of-emerging-email-threats-at-sea/ (last accessed Aug. 4, 2025).
[8] Case Study: Maersk's Response to NotPetya, https://sosintel.co.uk/case-study-maersks-response-to-notpetya-how-cybersecurity-best-practices-mitigated-a-major-cyberattack/ (last accessed Aug. 4, 2025).
[9] International Chamber of Shipping, Cyber Security Onboard Ships Guidelines (2021), https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (last accessed Aug. 4, 2025).
[10] India Foundation, Navigating Legal Frontiers: Combating Cyber Piracy in the 21st Century (Mar. 5, 2025), https://indiafoundation.in/articles-and-commentaries/navigating-legal-frontiers-combating-cyber-piracy-in-the-21st-century/ (last accessed Aug. 4, 2025).

ISSN: 2582-6433

binding agreement that specifically makes GPS spoofing in the maritime sector illegal, and national laws frequently don't keep up with technological advancements[11].

Supply Chain Manipulation: The accuracy of digital records, such as electronic bills of lading and cargo manifests, is essential to maritime logistics. Cybercriminals take advantage of flaws in these systems to change documents, reroute cargo, or make smuggling easier. These actions challenge established legal classifications and standards of proof by obfuscating the distinction between cybercrime and conventional maritime fraud. Because a breach in one node can spread throughout the supply chain, the danger is increased by the interdependence of port, customs, and logistics systems.

III. CASE STUDIES

The case studies that follow each highlight different threat vectors, operational effects, and legal issues at critical junctures in maritime cybersecurity. These instances highlight the need for strong, enforceable legislative frameworks and the susceptibility of the world's shipping infrastructure to cybercriminal exploitation.

A. The 2017 Maersk Breach: A Paralysis of Global Logistics

The NotPetya ransomware attack, which started out targeting Ukrainian companies using hacked accounting software, quickly expanded throughout Maersk's global IT infrastructure in June 2017[12]. The company's container booking, tracking, and port terminal activities were paralyzed for more than 10 days by the infection, which encrypted data on over 49,000 laptops and more than 1,000 vital programs[13]. Despite not being the main target, Maersk suffered losses of over $300 million as a result of the attack, underscoring the disastrous effects of inadequate cybersecurity measures in a globally integrated sector. In particular, the lack of explicit culpability provisions for third-party victims of state-sponsored cyber attacks was one of the holes in international legal frameworks that the breach revealed[14].

[11] O. Melnyk, Cybersecurity in Maritime Transport: An International Perspective on Legal Regulation, Lex Portus, vol. 11, no. 1, pp. 11–13 (2025),
[12] Case Study: Maersk's Response to NotPetya, SOS Intelligence (Oct. 18, 2024), https://sosintel.co.uk/case-study-maersks-response-to-notpetya-how-cybersecurity-best-practices-mitigated-a-major-cyberattack/ (last accessed Aug. 4, 2025).
[13] Collateral Damage Case Study – Maersk, Cyber UK (n.d.), https://cyber.uk/areas-of-cyber-security/cyber-security-threat-groups-2/collateral-damage-case-study-maersk/ (last accessed Aug. 4, 2025).
[14] International Maritime Organization, Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/ Rev.2 (June 7, 2017),

ISSN: 2582-6433

B. Port of San Diego: Disruption in Administration (2018)

Iranian hackers used the SamSam virus to launch a ransomware attack against the Port of San Diego in September 2018[15]. Vessel operations were not immediately impacted by the hack, which mainly interfered with administrative activities like business services and public records systems. The incident showed how even non-critical IT systems may act as entry points for more disruptive cyber assaults, even though the port was able to retrieve data from backups and did not pay the ransom. One enduring weakness in port cybersecurity is the absence of network segmentation between operational and administrative systems[16].

C. Shahid Rajaee Port in Iran (2020): The Realization of Geopolitical Risk

Operations at Iran's vital Shahid Rajaee port were affected in May 2020 by a cyberattack that was generally ascribed to a foreign state entity. Internal tracking systems were the target of the attack, which resulted in major backups and delays in operations.[17] The attack demonstrated the susceptibility of vital marine infrastructure to geopolitical cyber conflict and the limitations of current international law in attributing and responding to such acts, notwithstanding Iranian officials' claims that the problem had been contained.

When taken as a whole, these incidents highlight recurrent weaknesses, including inadequate firewall segmentation, delayed system updates, and phishing and social engineering as the main attack vectors[18]. They also reveal a legal gap in maritime cybersecurity, including ambiguous culpability for collateral harm, jurisdictional ambiguity, and a dearth of legally binding international standards to prevent, prosecute, or address cybercrimes in this area.[19] Some of these issues are addressed in the International Maritime Organization's (IMO) cyber risk management recommendations, however their applicability is limited by the fact that they are not legally enforceable.

[15] Port of San Diego hit by a ransomware attack, Maritime Cyber Security (Sept. 3, 2018), https://maritimecybersecurity.nl/incident/B3Kzw45oVX (last accessed Aug. 4, 2025).
[16] Ransomware Casts Anchor at the Port of San Diego, Infosecurity Magazine (Oct. 1, 2018), https://www.infosecurity-magazine.com/news/ransomware-casts-anchor-at-the/ (last accessed Aug. 4, 2025).
[17] Israel linked to cyber attack on Iranian port, Industrial Cyber (July 19, 2022), https://industrialcyber.co/news/israel-linked-to-cyber-attack-on-iranian-port/ (last accessed Aug. 4, 2025).
[18] O. Melnyk, Cybersecurity in Maritime Transport: An International Perspective on Legal Regulation, 11 Lex Portus 11 (2025),
[19] International Maritime Organization, Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.2 (2017), 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

ISSN: 2582-6433

IV. LEGAL FRAMEWORK: INDIA AND INTERNATIONAL NORMS

As nationally and internationally, the legislative framework governing maritime cybersecurity is disjointed. India's strategy is still primarily reactive and non-specialized, even though international organizations and a few states have started to require proactive cyber risk management.

A. The Legal Environment in India

There is currently no specific maritime cybersecurity law in India. Rather, legal protection is dispersed among a number of tools, none of which fully addresses the particular vulnerabilities of the industry.

a) Information Technology Act, 2000:

By default, marine businesses are covered by the IT Act, India's founding cyber law. Unauthorized access, destruction, or interference with computer systems including those used for cargo tracking, port logistics, and ship navigation are punishable under Section 43[20]. While Section 66C specifically targets identity theft a clause pertinent to phishing attempts on port employees or shipping business personnel Section 66 criminalizes hacking with intent to cause harm[21]. Nevertheless, the marine industry was not considered in the formulation of these rules, and Indian courts have not yet tested their applicability to cyber occurrences at sea.

b) The Bharatiya Nyaya Sanhita:

BNS has provisions on criminal conspiracy (Section 61) and cheating (Section 316), which may theoretically be applicable to data tampering or maritime cyber-fraud. The BNS, like the IT Act, is not sector-specific, though, and it doesn't specifically address the operational effects or technical subtleties of marine cybercrime.

c) The Digital Personal Data Protection Act of 2023[22]:

The DPDPA will require "data fiduciaries" possibly including port authorities and shipping companies to protect personal data from breaches and illegal access once it is fully implemented. Despite the Act's privacy focus, the marine industry may benefit indirectly from its security and breach notification provisions.

d) Guidelines from the Directorate General of Shipping (DGS):

The DGS periodically publishes operational advisories on cybersecurity, although these are not

[20] Information Technology Act, 2000, § 43, No. 21 of 2000, Acts of Parliament, 2000 (India),
[21] Information Technology Act, 2000, § 66, No. 21 of 2000, Acts of Parliament, 2000 (India),
[22] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India),

ISSN: 2582-6433

legally binding and have no legal authority[23]. Indian ports and shipping lines are not currently required by law to implement basic cybersecurity requirements, carry out routine audits, or notify a centralized maritime authority of issues.

B. Framework for International Law and Policy

Although there are differences in the legal responses to maritime cyber risk around the world, some countries and international organizations have taken more forceful stances.

a) International Maritime Organization:

With effect from January 1, 2021, the IMO's Resolution encourages administrations to make sure that cyber hazards are taken into account in safety management systems compliant with the International Safety Management (ISM) Code[24]. Although this is a step in the right direction, the resolution is not legally obligatory, and compliance is still optional[25]. Although the principle has been adopted into national regulations in many flag states, enforcement varies greatly.

b) UNCLOS, or the United Nations Convention on the Law of the Sea:

Although cybersecurity is not specifically covered by UNCLOS, flag states are required by Articles 94 and 217 to assure vessel safety and environmental protection[26], which may be interpreted to include dangers connected to cyberspace[27]. The Convention's usefulness as a tool for maritime cyber governance is, however, limited by its silence on digital dangers.

c) EU NIS Directive (2016) and NIS2 (2023):

The NIS Directive of the European Union requires incident reporting and risk mitigation strategies for operators of essential services, which includes port facilities[28]. These responsibilities are increased by the revised NIS2 Directive (2023), which mandates that operators of vital infrastructure, including ports, put in place thorough cybersecurity measures

[23] Directorate General of Shipping, Ministry of Shipping, Government of India
[24] International Maritime Organization, Resolution MSC.428(98), Guidelines on Maritime Cyber Risk Management (June 7, 2017), 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 (last accessed Aug. 4, 2025)
[25] GT Maritime, IMO, the ISM Code and Maritime Cyber Risk Management, https://www.gtmaritime.com/resource/imo-the-ism-code-and-maritime -cyber-risk-management/(last accessed Aug. 4, 2025).
[26] United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 3, arts. 94, 217,
[27] O. Melnyk, Cybersecurity in Maritime Transport: An International Perspective on Legal Regulation, 11 Lex Portus 11 (2025),
[28] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) 1 (EU).

ISSN: 2582-6433

and report serious occurrences[29]. Although these rules are not immediately enforceable outside of the EU, they set a high standard for maritime cybersecurity.

d) The US Coast Guard's 2020 Maritime Cybersecurity Plan

It mandates that port operators create and put into place risk-based cybersecurity mitigation plans, which include incident response procedures[30]. One major worldwide issue is the continuous discrepancy between enforceable mandates (like EU directive[31]) and soft law guidance (like IMO resolutions). Cross-border collaboration and enforcement are made more difficult by India's non-ratification of some international marine accords[32].

V. JURISDICTIONAL CHALLENGES IN MARITIME CYBERCRIME

International collaboration and national legal systems are bewildered by the distinct set of jurisdictional, evidential, and liability issues that maritime cybercrime poses. Because the marine industry is essentially global, technologically linked, and outsourced, these barriers attribution, high-seas jurisdiction, cross-border legal aid, and private entity liability are particularly noticeable in this industry.

a) Attribution: The Mysterious Offender

Phishing and malware campaigns are examples of cyberattacks that commonly use fake IP addresses, anonymizing networks, or hacked third-party systems in the maritime domain. It is extremely difficult to assign assaults to certain nation-states, cyber collectives, or even individual actors with any level of legal certainty because of this obfuscation[33]. The process of determining responsibility is made more difficult by the deliberate destruction of digital evidence and the technical complexity of digital forensics. These difficulties obstruct not just criminal prosecution but also the formulation of focused policy or diplomatic solutions[34].

b) High Seas Jurisdiction: The Boundaries of Flag State Power

Ships on the high seas fall within the exclusive jurisdiction of their flag state, as stated in Article 92 of the United Nations Convention on the Law of the Sea (UNCLOS)[35]. However, land-

[29] 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 (NIS2 Directive), 2022 O.J. (L 333) 80 (EU).
[30] US Coast Guard, Maritime Transportation Security Act (MTSA) Related Cyber Risk Management Policy, https://www.uscg.mil/cyber/ (last accessed Aug. 4, 2025).
[31] **Directive (EU) 2022/2555**, 2022 O.J. (L 333) 80
[32] International Maritime Organization, supra note 27.
[33] Kristen E. Eichensehr, The Law and Politics of Cyberattack Attribution, 67 UCLA L. Rev. 520, 522 (2020)
[34] O. Melnyk, Cybersecurity in Maritime Transport: An International Perspective on Legal Regulation, 11 Lex Portus 11, 13 (2025),
[35] United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 3, art. 92,

ISSN: 2582-6433

based infrastructure servers, cloud platforms, or even port IT systems located in countries different from the flag state are frequently the source of maritime cybercrimes. 4. Because of this discrepancy, cyber incidents involving actors completely unrelated to the vessel itself and spanning national borders cannot be adequately handled by the conventional maritime legal premise of flag-state exclusivity. The uncertainty around whether Article 92 covers adjudicative (judicial), prescriptive (law-making), or merely enforcement jurisdiction only serves to increase the confusion and creates significant gaps in the hunt for cybercriminals who take advantage of these loopholes[36].

c) Legal Aid Across Boundaries: The Budapest Convention Deficit

Strong international legal cooperation is necessary for the efficient investigation and prosecution of marine cybercrime. The only legally binding international agreement that addresses cybercrime expressly is the Council of Europe Convention on Cybercrime (Budapest Convention, 2001), which provides procedures for extradition, evidence sharing, and mutual legal assistance among signatory states[37]. Nevertheless, India does not have a strong network of Mutual Legal Assistance Treaties (MLATs) with other maritime nations and is not a party to the Budapest Convention[38]. This severely restricts India's ability to gather international evidence, speak with witnesses, or track down hackers working outside, especially when it comes to phishing, data theft, or ransomware assaults against ships flying the Indian flag or port infrastructure.

d) Liability of Private Entities: The Outsourcing Conundrum

To handle crucial activities, port owners and shipping lines are depending more and more on cloud service providers, logistics platforms, and outsourced IT suppliers. Determining responsibility becomes difficult in the event of a breach, such as a successful phishing attempt that results in ransomware infection or data exfiltration. The allocation of accountability among shipping firms, port authorities, and their providers is complicated by contractual indemnity agreements, varying standards of care, and jurisdictional inconsistencies in cybersecurity law. This problem is made worse by India's lack of sector-specific legislative responsibilities, which leaves regulators and victims without obvious legal options in the case of systemic failure[39].

[36] Giuliana Lampo, Defining the Scope of Exclusive Flag-State Jurisdiction Under Art. 92 UNCLOS, 82 ZaöRV 195, 201–21 (2022),
[37] Council of Europe Convention on Cybercrime, Nov. 23, 2001, ETS No. 185,
[38] Cybercrime and Legal Challenges, Lawful Legal (June 24, 2025), https://lawfullegal.in/cyber-crime-and-legal-challenges/ (last accessed Aug. 4, 2025).
[39] CyberPeace, Safeguarding the Seas: Cyber Resilience in the Maritime Industry (May 5, 2025), https://www.cyberpeace.org/resources/blogs/safeguarding-the-seas-cyber-resilience-in-the-maritime-industry (last accessed Aug. 4, 2025).

ISSN: 2582-6433

VI. REGULATORY RECOMMENDATIONS

Strong, proactive, and enforceable regulatory interventions are required due to the ongoing weaknesses in India's marine cybersecurity architecture as well as the jurisdictional and enforcement challenges mentioned above. If put into practice, the following suggestions might significantly increase India's marine industry's resistance to cyberattacks and bring it into line with global best practices:

a) Create a National Maritime Cybersecurity Authority:

India ought to establish a centralized maritime cyber regulator with the legally enforceable power to establish and implement cybersecurity guidelines for shipping businesses and ports[40]. This organization would provide as a single point of oversight for a field that is currently dispersed among several agencies by issuing required incident reporting rules, keeping an eye on compliance, and coordinating responses during cyber crises. One A specialized authority might also act as a clearinghouse for industry-specific threat intelligence and best practices, enabling stakeholders to share information promptly.

b) Require Regular Cyber Risk Assessments:

Regular, independent cybersecurity risk assessments should be mandated for all ports, big and small, with an emphasis on staff knowledge, phishing defense, and simulation exercises. By identifying weaknesses in operational technology, digital infrastructure, and human factors, these evaluations would guarantee that cybersecurity is approached as a continuous procedure rather than a one-time compliance activity[41]. The results ought to guide focused employee training initiatives and ongoing incident response plan improvement.

c) Ratify the Budapest Convention on Cybercrime:

It is long overdue for India to ratify the Budapest Convention on Cybercrime, also known as the Council of Europe Convention on Cybercrime. Ratification will facilitate cross-border evidence collection, allow for organized international collaboration in cybercrime investigations, and strengthen India's ability to prosecute cybercriminals operating outside of its borders. Such collaboration is necessary for efficient attribution, prosecution, and deterrent because marine cybercrime is multinational in nature.

d) Make Cyber Insurance Mandatory for Shipping Companies:

[40] O. Melnyk, Cybersecurity in Maritime Transport: An International Perspective on Legal Regulation, 11 Lex Portus 11, 18 (2025)

[41] Cyril Amarchand Mangaldas, Fighting Cybercrime: Global UN Convention on the Anvil (Sept. 2024), https://corporate.cyrilamarchandblogs.com/2024/09/fighting-cybercrime-global-un-convention-on-the-anvil/ (last accessed Aug. 4, 2025).

ISSN: 2582-6433

In addition to providing victims with access to financial resources for recovery and remediation, requiring cyber insurance for port operators and shipping businesses would encourage proactive risk management. In response, insurance companies would probably mandate that policyholders implement minimum cybersecurity safeguards, establishing a process driven by the market to improve industry standards. Guidelines for minimum coverage and maritime-specific claims procedures should be included in addition to this requirement.

e) Establish Penal Provisions for Cybersecurity Negligence :

By adding particular sanctions for failing to secure maritime digital infrastructure to the Merchant Shipping Act of 1958, it would serve as a powerful disincentive to become complacent. Provisions might cover anything from criminal culpability in circumstances of egregious negligence resulting in major operational disruption or data breaches to fines for procedural errors. In addition to decreasing uncertainty in liability issues, clear statutory responsibilities would also make it clearer how port authorities, shipping corporations, and their IT vendors share responsibility.

When combined, these steps would not only fill in significant gaps in India's maritime cybersecurity framework, but they would also show the world that India is dedicated to protecting one of the most important commercial corridors in the world. It is impossible to overestimate the importance of regulatory reform given the growing digital interconnectivity of the maritime industry. The only practical way to reduce the changing threats that cybercriminals offer to international marine trade is through proactive, enforced, and cooperative governance.

VII. CONCLUSION

The continuous digital revolution of the marine industry has brought about previously unheard-of operational efficiencies, but it has also made ports, shipping companies, and international supply chains vulnerable to advanced cyberthreats. The shortcomings of India's current legal system, which relies on general IT rules and voluntary advice, are becoming more and more obvious as the country moves forward with its marine objectives through programs like Sagarmala and the marine India Vision 2030. Supply chain attacks, ransomware, and phishing attempts directed at the marine industry highlight the intricacy and worldwide scope of these threats. The coordinated, cross-border nature of marine cybercrime cannot be adequately addressed by the fragmented legislative provisions currently in place. Critical national infrastructure is at risk due to jurisdictional ambiguity, gaps in international collaboration (made worse by India's non-ratification of the Budapest Convention), and a lack of sector-

ISSN: 2582-6433

specific cybersecurity obligations[42].

The International Maritime Organization's standards serve as a starting point, but their effectiveness in promoting compliance is limited by the fact that they are not legally obligatory. Adopting a uniform marine cybersecurity policy that aligns national legislation with global best practices, creates transparent accountability for public and commercial parties, and implements strong deterrent mechanisms is imperative for India. For all maritime organizations, this policy should require frequent risk assessments, incident reporting, and baseline cybersecurity standards. India can only ensure its maritime future if it treats cyber resilience as a strategic priority and aligns regulatory ambition with the reality of international cyber threats.

[42] Cyril Amarchand Mangaldas, Fighting Cybercrime: Global UN Convention on the Anvil (Sept. 2024), https://corporate.cyrilamarchandblogs.com/2024/09/fighting-cybercrime-global-un-convention-on-the-anvil/ (last accessed Aug. 4, 2025).