THE CHALLENGE OF "SILENT CYBER" IN MARITIME LOGISTICS

Lushita Banik, LLM (BL), Amity University Noida

ABSTRACT

Now shaping the sector, digital tools have become routine across ships, harbours, and shipping chains - automation runs deep, satellite tracking guides routes, and data flows link every step. Efficiency gains come at a cost: lines between online threats and real-world harm grow thin as systems connect. Hidden exposure emerges when cyber incidents slip through policy wordings - an uncertainty known as "silent cyber," where coverage stays undefined by design.[1] Not covered outright, yet not ruled out either, these gaps unsettle standard marine insurance terms. Seaworthiness rules now face pressure under outdated statutory language.[2] Legal strain becomes visible when comparing India's 2000 IT Act against modern contractual responses like the BIMCO Cyber Security Clause from 2019.[3] Outdated laws meet new clauses with little alignment, leaving liability unclear. Uncertainty lingers where statutes stop short and contracts stretch further. Beginning with legal doctrine and academic sources, this piece examines whether digital vulnerabilities can undermine a ship's seaworthiness.[4] Cyber-caused physical harm often slips through gaps in established marine coverage models. Existing rules fail to properly manage online dangers within smart harbours like JNPT.[5] Attention turns to the need for updated standards when technology reshapes port systems. Incorporating digital threat oversight into shipping laws appears necessary. So does revising insurance terms to reflect modern hazards. Safety and durability in ocean logistics depend on these shifts. Without them, risks grow unchecked.

[1] Ruth Taplin, Cyber Risk, Intellectual Property Theft and Cyberwarfare: Asia, Europe and the USA (Routledge 2020)
[2] Feng Wang, The Warranty of Seaworthiness and Cyber Risk of Unmanned Ships, *J. Bus. L.* (2020).
[3] Baltic & Int'l Maritime Council (BIMCO), Cyber Security Clause 2019, available at: https://www.bimco.org (last visited Mar 11, 2026)
[4] M.B. Kao, Cybersecurity in the Shipping Industry and English Marine Insurance Law, 45 *Tul. Mar. L.J.* (2020).
[5] Jawaharlal Nehru Port Authority, Digital Port Initiatives, available at: https://www.jnport.gov.in (last visited Mar 11, 2026)

1. Introduction

Although sea transport once dealt mainly with tangible dangers like bad weather, crashes at sea, theft by pirates, or broken equipment, its challenges now extend beyond the physical world. Digital advances in international shipping have reshaped how risks emerge and spread across operations. Ships today depend on networks - navigation via satellites, software that handles freight, and tools allowing distant oversight of vessel functions.[6] Because of this shift toward automation, weaknesses have appeared where hackers might strike. Even as performance improves through technology, unseen threats grow alongside it.

Not often discussed, yet increasingly relevant, lies a gap in many standard marine insurance contracts - cyber risks sneak through without clear mention.[7] These agreements typically respond to tangible harm, though they rarely clarify if digital triggers behind such harm count. When systems fail due to hacking or malware, ambiguity grows about who bears the cost. Policies written before today's threat landscape took shape now face scrutiny under modern attack patterns. Even when equipment burns because of a compromised network, insurers hesitate. The absence of explicit terms leaves room for debate after disaster strikes.

In places like India's Jawaharlal Nehru Port Trust - where automation runs deep - digital tools handle everything from container movements to temperature controls, ship schedules, and border checks. When hackers breach these setups, real-world harm follows: imagine cold boxes failing because software settings are tampered with, or ships misrouted through corrupted data streams.

Even with new dangers appearing, much of the legal structure around shipping still feels old-fashioned. Instead of addressing digital dangers, rules like those in the Marine Insurance Act usually deal only with tangible sea-related hazards. Because of this split, oversight for ships often misses what happens online. As a result, laws about oceans and data rarely connect where they should.

A close look at quiet digital dangers within shipping reveals growing legal questions. When ships face unseen online threats, rules struggle to keep pace. India’s 2000 tech law does not

[6] Peter Zhang & Ling Tang, Ship Management: Theory and Practice (Routledge 2021).
[7] A.R. Katsimani, Cyber-Attacks as a Covered Risk in Marine Insurance (2025).

fully meet modern maritime needs. Meanwhile, BIMCO introduced a cybersecurity clause in 2019 to fill part of that space. Seaworthiness now includes more than hull strength or cargo safety - digital readiness matters too. Ship operators may find themselves exposed where laws lack clarity. Insurers, although involved, often rely on outdated frameworks. Where one rule ends, another begins - but mismatched timing creates risk. Vessels might be judged fit yet still vulnerable through hidden system flaws. Laws written before widespread connectivity fail current demands. Responsibility blurs when technology gaps exist between policy and practice. This misalignment shapes outcomes after incidents occur.

2. Digital Shifts and Online Threats in Sea Transport

Although shipping once relied on traditional methods, new tools now shape how vessels move across oceans. Today's boats use devices like Automatic Identification System (AIS) to share location data without constant radio contact. Electronic Chart Display and Information System (ECDIS) replaces paper maps with screens that update in real time during voyages. Bridge operations link multiple functions into unified control centres for better coordination. Instead of manual logs, port activities depend on software managing container movements precisely. Digital records have taken over, where paperwork used to slow down freight processing. Automation quietly runs much of what keeps global trade flowing at terminals.[8]

Though such advances improve how systems run, weaknesses emerge at the same time - openings attackers might use. Cyber threats find footing where progress creates complexity.

In their 2023 work, Schinas and Metzger point to a specific source of cyber risk at sea - emerging where three linked areas overlap.[9] This vulnerability does not stem from isolated systems, it appears through connections across domains. Each part influences the others, creating points of exposure that would otherwise remain separate. Interdependence becomes the pathway through which threats travel. As digital technologies embed into operations, new access routes form unintentionally. The meeting of these spheres introduces complexity often overlooked in standard assessments

1. Operational technology (OT) controlling vessel machinery and cargo systems

[8] Peter Zhang & Ling Tang, Ship Management: Theory and Practice (Routledge 2021).
[9] Olaf Schinas & Dimitrios Metzger, Cyber-Seaworthiness: A Critical Review of the Literature, *Marine Policy* (2023)

2. Information technology (IT) used for data management and logistics operations

3. Communication systems linking ships, ports, and logistics networks

When these systems come together, hacking can lead to real-world effects. Take cargo cooling units - cyber attackers might alter their settings, compromise navigation tools, or create delays in port operations through digital interference.[10]

One often-mentioned case dates back to 2017: the NotPetya incident that threw international freight systems into disarray, notably affecting Maersk's cargo logistics. Billions vanished due to digital failures - proof that virtual breaches can paralyze real-world distribution networks.[11]

Fake signals in navigation systems show up across various areas, making it possible to mislead tracking of ships.[12] Because of these cases, doubts grow over how safe sea travel really is, along with questions about consistent performance.

Cyber-seaworthiness has emerged as a key idea, following recent changes - scholars now argue vessels need strong digital safeguards to meet traditional standards of readiness.[13]

3. The Idea of Silent Cyber in Marine Insurance

For centuries, marine insurance has helped reduce dangers tied to sea travel. Usually, these policies respond to damage caused by events like heavy weather, accidents between vessels, or breakdowns of equipment.[14]

Still, rising cyber dangers have revealed weak spots in older insurance models.

When cyber threats aren't clearly covered in insurance contracts, confusion often follows - this gap is known as silent cyber.[15] Damage caused by digital attacks sometimes slips into

[10] Feng Wang, The Warranty of Seaworthiness and Cyber Risk of Unmanned Ships, *J. Bus. L.* (2020).
[11] Ruth Taplin, Cyber Risk, Intellectual Property Theft and Cyberwarfare: Asia, Europe and the USA (Routledge 2020).
[12] Michael Neo, The Rising Threat of Maritime Cyber-Attacks, Royal Australian Navy Sea Power Centre (2021).
[13] Özge Kara Balci & İrem Varan Samut, An Evaluation of Cyber-Worthiness and Related Factors in Maritime Safety, *J. Mar. Affs. & Shipping* (2024).
[14] Marine Insurance Act, 1963 (India).
[15] M.B. Kao, Cybersecurity in the Shipping Industry and English Marine Insurance Law, 45 *Tul. Mar. L.J.* (2020).

conventional categories, catching insurers off guard.

A sudden shift occurs when hackers alter cooling systems in transport units holding goods that decay easily. Spoilage follows, counted as tangible harm by shipping insurers. Yet the origin - an online breach - might fall outside stated protections.

Uncertainty of meaning leads to disagreements over responsibility, pitting insurance companies against their customers.

Beginning with a fresh perspective, Katsimani suggests silence around cyber dangers puts pressure on core ideas in marine coverage, since older contracts focused on physical sea perils instead of online vulnerabilities.[16] While built for storms and shipwrecks, those forms now face unseen digital disruptions. Though long-standing frameworks remain, they struggle when code - not waves - causes harm. Because digitized systems grow central to shipping, outdated terms appear increasingly misaligned. Yet even so, adaptation moves slowly across underwriting circles.

Besides tackling the problem, insurance providers more often add clauses that block cyber claims by default - coverage only applies if directly purchased. Though broad policies exist, they typically leave digital risks out unless flagged upfront.

4. BIMCO Cyber Security Clause 2019

A fresh approach to digital threats in maritime contracts emerged when Baltic and International Maritime Council (BIMCO) launched its 2019 Cyber Security Clause. While deals at sea evolved slowly, this addition slipped into agreements aiming to handle online vulnerabilities. Instead of waiting for disasters, companies began including it quietly alongside terms about cargo and timing. Though not mandatory, its presence signalled growing unease over hacking dangers. As ships rely more on connected systems, such clauses act like small shields woven into a larger legal fabric.

When it comes to safeguarding ship functions and data networks, those involved - owners, charterers, along with others bound by contract - are expected to apply suitable digital defences. How well these steps work often depends on how seriously each party takes their role in the

[16] A.R. Katsimani, Cyber-Attacks as a Covered Risk in Marine Insurance (2025).

process.

A breach qualifies as a cyber incident when it involves unapproved entry, interference, or harm targeting digital infrastructure - especially if sea-related activities face consequences.[17] While compromised systems or distorted networks count, only those impacting operational continuity matter here. Such events include intrusions, breakdowns, or corrupted information within technology used at sea.

The primary objectives of the BIMCO clause include:

1. Encouraging shipowners to adopt cybersecurity risk management practices

2. Who handles what when digital breaches occur gets sorted through agreements between involved organizations

3. Ensuring that cybersecurity measures are integrated into maritime operations

Certain clauses serve more to assign responsibility between parties than to enforce broad legal standards.

It seems clear from Dogan's work that the BIMCO clause acknowledges how tightly cybersecurity now ties into safe ship operations.[18] While once treated separately, digital threats are increasingly seen as risks on par with mechanical failure. Because of this shift, protections built around data and systems have gained weight in maritime standards. What stands out is not just awareness, but the move to embed such concerns directly into contractual terms. So instead of treating cyber issues as add-ons, they now shape core safety expectations.

The issue remains only partly addressed, even though the clause matters - its emphasis sits with contracts instead of actual protection. What persists is a gap between duty and defence, since coverage itself stays untouched by these terms.

5. Vessel Seaworthiness Meets Cybersecurity

Seaworthiness matters most at sea, shaping rules in shipping law and coverage policies. When

[17] M.B. Kao, Cybersecurity in the Shipping Industry and English Marine Insurance Law, 45 *Tul. Mar. L.J.* (2020).
[18] Faruk Dogan, Cyber-Worthiness in Shipping: Law, Regulation and Practice (Routledge 2026).

built right, kept well, on top of crew readiness, a ship meets the standard for open-water travel.

For years, evaluation of a ship's ability to handle sea conditions focused on:

1. Structural integrity of the vessel
2. Proper functioning of machinery
3. Adequate crew competence
4. Availability of safety equipment

Still, going digital has broadened what it means for a ship to be fit for sea.

Focusing on ship readiness, experts now link digital security to seaworthy conditions since weak systems risk navigation integrity. Despite traditional views, software flaws are seen as hazards equal to mechanical faults when assessing ocean travel fitness. Because hacking threats may disrupt operations at sea, some researchers classify strong defences as essential to safe voyages. As technology grows onboard, protection against online breaches becomes a factor in whether vessels meet safety standards. Instead of treating it separately, modern analysis treats cyber resilience like structural soundness in maritime contexts.

A ship relying on unsecured navigation tech could face intrusions distorting its route information or disrupting safety protocols meant to prevent crashes.[19]

When hackers hit cargo control networks, operations can stall - sometimes spoiling shipments. A breach might freeze logistics, delaying deliveries across regions.[20]

Starting fresh, Balci and Samut suggest weaving "cyber-worthiness" into maritime safety standards - so shipowners adopt strong digital safeguards.[21] Though subtle, the shift matters: security becomes a baseline, not an add-on. Instead of waiting for breaches, preparedness takes root early. Because risks evolve fast, static rules fall short. Therefore, adaptability gains weight within oversight systems. While some resist change, others see it as inevitable. Since vessels

[19] Feng Wang, The Warranty of Seaworthiness and Cyber Risk of Unmanned Ships, *J. Bus. L.* (2020).
[20] T. Michalopoulos, Cyberattack as a Covered Danger in Marine Insurance (2022).
[21] Özge Kara Balci & İrem Varan Samut, An Evaluation of Cyber-Worthiness and Related Factors in Maritime Safety, *J. Mar. Affs. & Shipping* (2024).

rely more on networks, weak links grow dangerous. Thus, proactive steps make sense - not just compliance after damage occurs.

Failing here might make a ship unfit for sea, leaving owners open to legal responsibility.

6. The Information Technology Act of 2000 and Its Role in Maritime Cyber Security

Starting off, India relies on the Information Technology Act of 2000 as its main legal framework for digital conduct. While focused on online actions, it specifically targets breaches like illegal entry into systems, stealing information, or disrupting operations.

Among the rules tied to maritime cybersecurity are these key elements:

1. Section 43: Liability for unauthorized access or damage to computer systems

2. Section 66: Criminal penalties for hacking and cyber fraud

3. Section 66B–66F: Offenses involving identity theft, cyber terrorism, and data breaches

Around digital crimes, the IT Act sets up legal pathways - yet its structure never focused on sea-based activities. Instead, offshore contexts fall outside its original blueprint.[22]

Because of this, the law overlooks key matters at sea like:

1. Cyber-Induced Vessel Unseaworthiness

2. Cyber Risks Affecting Marine Insurance

3. Liability allocation among shipowners, charterers, and port operators

A space forms where laws on digital crimes meet sea-based safety efforts without clear rules. This divide leaves gaps that neither field fully addresses.

7. The Legal Divide Between IT Act and Maritime Law

Cyber law meets maritime law in ways that most legal systems still fail to clarify.

[22] D. Dadiani, Cyber-Security and Marine Insurance (World Maritime University 2018).

Though the Information Technology Act deals with crimes in cyberspace, rules at sea center on safe operations, coverage claims and trade ties. Shipping regulations care less about digital wrongdoing, more about vessel conduct, financial protection, business duties under wave-bound frameworks.

Here lies a split that brings multiple hurdles for regulation

1. Lack of Standards for Cyber Seaworthiness - A vessel's duty to remain seaworthy does not, under current Indian maritime regulations or the Information Technology Act, clearly include maintaining cyber defences.

So long gaps in digital defences often go unnoticed until something breaks.

2. Insurance Coverage Uncertainty - Not covered by standard maritime insurance, cyber threats can hit vessel operators where it hurts - through unforeseen costs tied to digital breaches. While physical damage falls under typical coverage, glitches sparked by hacking do not.

3. Jurisdictional Complexity - Cross-border hacking incidents complicate legal responses due to differing national laws. Jurisdictional overlaps slow down accountability efforts across regions.

A ship docked at an Indian harbour might face digital threats launched remotely from abroad.

4. Fragmented Regulatory Framework - Maintained through global agreements like the SOLAS Convention, maritime safety operates separately from cybercrime regulation, which instead follows domestic statutes including the IT Act.[23]

Fragments like these tend to leave rules uneven across regions.

8. Automated ports like JNPT face new challenges

For automated terminals like Jawaharlal Nehru Port Trust (JNPT), silent cyber threats matter more than often acknowledged. While systems run without human input, unseen vulnerabilities can still emerge - quietly, yet with impact.

[23] International Convention for the Safety of Life at Sea (SOLAS), Nov. 1, 1974, 1184 U.N.T.S. 278.

Operating through advanced software, JNPT manages freight via self-guided terminal operations alongside digital paperwork handling. While automation drives efficiency, data-based tracking supports real-time shipment monitoring across ports.[24]

A breach in these systems might halt port activities, while also harming shipments.

For example:

1. Fooling a system might let someone change how cold shipping containers stay

2. Malware could disable automated cranes

3. Attackers could falsify container tracking data

A single event could lead to actual harm to goods, setting off claims where hidden digital threats play a role.

Clearly, maritime logistics demands cohesive approaches to digital oversight. A unified system becomes essential when managing online risks across supply chains. Where operations span global networks, fragmented rules create openings for threats. Stronger coordination helps close gaps in how data is protected at sea and on land. Without alignment between policies, vulnerabilities multiply quietly beneath the surface.

9. Policy Recommendations

Fixing the quiet digital threat means updating laws through joint efforts across agencies. While rules adapt slowly, changes must happen together to close gaps. Because one shift affects another, timing matters just as much as design. Without alignment, updates risk falling short or causing new issues elsewhere.

1. Cybersecurity Meets Ship Readiness

Maritime regulators should recognize cybersecurity as a component of vessel seaworthiness.

Facing new threats, shipowners might need to adopt ways of handling cyber risks

[24] E.J. Eftestøl, A. Bask & M. Huemer, Towards a Zero-Emissions and Digitalized Transport Sector: Law, Regulation and Logistics (2024).

systematically.

2. Updating Marine Insurance Policies

When insurance systems fail to name cyber threats outright, confusion follows. Clarity comes only when policies clearly define digital dangers. Unless coverage spells out these exposures, uncertainty remains. Where terms stay vague, gaps appear in protection. Only precise language closes the loophole. Ambiguity fades once wording takes aim at online hazards directly.

3. Aligning Rules for Sea and Internet

National cyber legislation should incorporate provisions addressing maritime cyber risks.

4. Strengthening International Cooperation

Across borders, cyber dangers touch shipping networks deeply. Because of this reality, nations must work together closely - only then can rules truly matter.

10. Conclusion

Not every change brings progress - digital shifts in shipping reveal hidden weaknesses testing old laws. When software fails silently, harm follows without clear liability under current policies.

A mismatch exists where India's Information Technology Act of 2000 does not align clearly with tools like the BIMCO Cyber Security Clause introduced in 2019. Because of this disconnect, combining legal frameworks becomes necessary when addressing cyber risks at sea. While one governs digital systems nationally, the other applies selectively within shipping operations globally. Where legislation lags, industry standards step in - yet they lack enforceability under domestic law. Merging these domains could close vulnerabilities now exploited through weak oversight.

With automation rising at hubs like JNPT, safeguarding systems grow essential within port oversight. Though technology advances rapidly, protecting data flows cannot lag behind in shipping operations. Since digital tools spread across terminals, security demands keep shifting alongside them. When machines handle more tasks, human oversight adapts - yet risks evolve just as fast. Because networked infrastructure expands, weak points emerge where few expect

them. While efficiency improves through code, vulnerabilities often hide inside connected devices. As control shifts to software platforms, preparedness shapes how well ports withstand attacks.

Should laws fail to tackle digital safety at sea, protection gaps may persist. When rules around cyber-readiness stay unchanged, shipping networks face ongoing risks. Unless insurers adapt policies, weaknesses linger. With oversight bodies working apart, hazards multiply. Unchecked, these flaws can halt movement across international trade routes.

References

Articles

- O. Schinas & D. Metzger, Cyber-Seaworthiness: A Critical Review of the Literature, 152 *Marine Policy* 105738 (2023), https://doi.org/10.1016/j.marpol.2023.105738.

- F. Dogan, Cyber-Worthiness in Shipping: Law, Regulation and Practice (Routledge 2026).

- Ö. Kara Balci & İ. Varan Samut, An Evaluation of Cyber-Worthiness and Related Factors in Maritime Safety and Maritime Security, *Mar. Affs. & Shipping* (2024).

- M. S. Karim, Maritime Cybersecurity and the IMO Legal Instruments: Sluggish Response to an Escalating Threat, 144 *Marine Policy* 105220 (2022), https://doi.org/10.1016/j.marpol.2022.105220.

- R. Hopcraft & K. M. Martin, Effective Maritime Cybersecurity Regulation: The Case for a Cyber Code, 14 *J. Indian Ocean Region* 218 (2018).

- J. Choi & J. Qi, Regulating Cyber Security of Maritime Autonomous Surface Ships: New Challenges and Improvements, 16 *J. E. Asia & Int'l L.* 423 (2023).

- F. Wang, The Warranty of Seaworthiness and Cyber Risk of Unmanned Ships, *J. Bus. L.* 245 (2020).

- S. Cooper, Cyber Risk, Liabilities and Insurance in the Marine Sector, in *Maritime Liabilities in a Global and Regional Context* 201 (Routledge 2018).

- A. R. Katsimani, Cyber-Attacks as a Covered Risk in Marine Insurance (Univ. of Piraeus Thesis 2025).

- C. Kapalidis, Cyber Risk Assessment in the Maritime Transport Sector: Ships, Ports and Port Systems (Loughborough Univ. Doctoral Thesis 2025).

- N. A. R. Al Ali, A. A. Chebotareva & V. E. Chebotarev, Cyber Security in Marine Transport: Opportunities and Legal Challenges, 35 *Pomorstvo* 245 (2021).

- M. Neo, The Rising Threat of Maritime Cyber-Attacks: Maritime Cyber-Security Preparedness, *Royal Australian Navy Sea Power Series* (2021).

Legal Instruments, Statutes and Government Institutions

- Information Technology Act 2000, No. 21 of 2000, (India).
- Marine Insurance Act, 1963, No. 11 of 1963, (India).
- Baltic & Int'l Maritime Council (BIMCO), Cyber Security Clause for Time Charter Parties 2019 (2019).
- International Maritime Organization (IMO), Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3 (2017).
- International Convention for the Safety of Life at Sea (SOLAS), Nov. 1, 1974, 1184 U.N.T.S. 3.
- Jawaharlal Nehru Port Authority, Digital Port Initiatives.