International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Threats at Sea: The Urgent Need for Digital Resilience in Maritime Operations

Dr. Meena Ravi Shankar[1], Mr. Pavan Sai Chand Ananta[2], Mr. Dhruv Manral[3]

[1]Hr & Soft Skills Faculty, The Great Eastern Institute Of Maritime Studies
[2]Electrical Officer, The Great Eastern Institute Of Maritime Studies
[3]Trainee Electro Officer, The Great Eastern Institute Of Maritime Studies

Abstract

The maritime industry is becoming rapidly more digital — from navigation and collision avoidance (GPS, ECDIS, AIS), to engine control, cargo management, port logistics, satellite communications (VSAT), and supply chain tracking. These technologies improve efficiency, safety and cost-saving. However, they also expose vessels, ports, and related infrastructure to cyber-risks: unauthorized access, spoofing, malware, ransomware, insider threats, data theft, system failures. A successful cyberattack may lead not just to financial losses and delays, but also threats to lives, environmental damage, loss of cargo, reputational damage, and even escalation of geopolitical tension.

To address this, regulatory and formal standards need amendments and updating. Key areas include:

Strengthening classification rules: e.g. mandates for cyber-resilience of ship systems (on board OT as well as IT). Mandating type-approval testing of automation and navigational systems.

Requirements for continuous risk assessments, incident detection & response plans, crew training in cybersecurity. Updating guidelines in IMO / ISM Code to explicitly cover cyber events, make compliance mandatory rather than advisory.

Harmonizing international standards and reporting, so all vessels and ports meet certain minimal cybersecurity hygiene, encryption, access control, supply chain security.

KEYWORDS: Encryption-process of converting readable data (plaintext) into an unreadable format (cipher text) to protect it from unauthorized access

1. Introduction

Maritime operations have rapidly digitized, connecting ships, ports, logistics, navigation and supply-chain partners into a global, heterogeneous cyber-physical ecosystem. This connectivity brings operational efficiencies but also exposes the maritime sector to a wide spectrum of cyber threats — from ransomware and supply-chain compromises to GNSS (GPS) spoofing and AIS manipulation.

This paper synthesizes literature, incident analyses and industry guidance to (1) map the contemporary maritime cyber threat landscape, (2) examine emblematic case studies (NotPetya/Maersk; AIS/GNSS spoofing events), (3) analyze vulnerabilities in shipboard and port systems, and (4) propose a layered, practical framework to build digital resilience across technical, organizational and regulatory domains.

The recommendations combine network segmentation, robust cyber hygiene, incident response preparedness, seafarer training, and multi-stakeholder information sharing — embedded within Safety Management Systems (SMS) and regulatory compliance. Key findings emphasize that digital resilience is not optional but integral to maritime safety, environmental protection, and global trade continuity. IMO+1

The maritime sector underpins over 80% of global trade by volume and increasingly depends on digital systems — Electronic Chart Display and Information Systems (ECDIS), Automatic Identification System (AIS), satellite navigation (GNSS), port terminal operating systems (TOS), and cloud-based logistics platforms. As connectivity increases, so does exposure to cyber threats that can disrupt navigation, cargo handling, safety systems and commercial operations. In response, the International Maritime Organization (IMO) required cyber risk management to be integrated into Safety Management Systems (Resolution MSC.428(98), adopted 2017), mandating ship-owners and operators to assess and manage cyber risk. However, despite regulatory progress and industry guidance, high-impact incidents and numerous documented vulnerabilities demonstrate persistent gaps in preparedness and resilience. IMO+1

This paper explores the contemporary threat landscape, examines high-profile incidents, and offers a set of strategic and operational measures aimed at improving maritime cyber resilience. The target audience includes maritime operators, shipboard teams, port authorities, regulators, and cybersecurity practitioners.

2. Background and Context

2.1 The Changing Maritime Technology Stack

Modern merchant vessels and port terminals integrate multiple interdependent systems:

- **Navigation and bridge systems:** ECDIS, automatic identification system (AIS), GPS/GNSS receivers.
- **Communication systems:** Satellite communication (VSAT), shore-to-ship links, email and office networks.
- **Propulsion and automation:** Engine and power management systems, integrated bridge systems, dynamic positioning on specialized vessels.
- **Cargo and terminal systems:** Terminal operating systems (TOS), container management, and automated stacking cranes.
- **Enterprise IT:** ERP systems, email, supply-chain platforms, and third-party vendor services.

2.2 Why the Maritime Sector Is Attractive to Attackers

Attackers target maritime assets for multiple reasons: financial gain (ransomware, fraud), espionage (cargo manifests, routes), operational sabotage (disruption of trade), and even geopolitical effects (targeting critical infrastructure during conflicts). Several characteristics make maritime attractive to attackers:

- **Heterogeneous systems** with long lifecycles and varying security postures.
- **Limited crew cybersecurity training** and high staff turnover.
- **Global supply chains** and numerous third-party vendors with inconsistent controls.
- **High-stakes outcomes** (safety, environmental damage) that may pressure victims to pay ransoms.

2.3. Threat Types and Attack Vectors

2.3.1 Malware and Ransomware

Ransomware can propagate through corporate networks and into operational systems, encrypting files and disabling services. Supply-chain malware can be introduced via trusted software updates or third-party tools.

2.3.2 GPS/GNSS Spoofing and Jamming

Spoofing involves feeding false positioning signals to GNSS receivers, causing vessels to compute incorrect locations. Jamming denies receivers the signals entirely. Both can lead to navigation errors, dangerous manoeuvres, or concealment of vessel movements.

2.3.3 Phishing and Social Engineering

Crew members and shore staff remain prime targets for phishing emails, malicious links, and credential theft. Successful social engineering may provide attackers initial entry to corporate networks.

2.3.4 Unauthorized Access and Weak Network Segmentation

Poorly segmented networks allow attackers to pivot from business IT into OT systems. Default credentials, outdated firmware, and exposed services increase risk.

2.3.5 Data Theft and Espionage

Cargo manifests, schedule information, and routing details have value to criminals and state actors. Data theft may facilitate piracy, theft at berth, or competitive intelligence gathering.

2.3.6 Insider Threats

Insiders with privileges — malicious or negligent — can introduce malware, misconfigure systems, or exfiltrate data.

2.4. Vulnerability Analysis

2.4.1 Vulnerabilities Specific to Maritime Systems

- **Legacy systems & heterogeneous vendors:** Ships commonly have equipment from multiple vendors with variable patching lifecycles and inconsistent security.
- **Lack of network segmentation:** IT and Operational Technology (OT) networks are sometimes insufficiently separated, enabling malware to cross into navigation or engine control systems.
- **Inadequate authentication for maritime broadcast systems:** AIS and many GNSS services lack cryptographic authentication, making them susceptible to spoofing.
- **Human factors:** Limited crew cybersecurity training and weak shore-to-ship governance raise exposure.
- **Regulatory compliance gaps:** While IMO mandated SMS integration, implementation and verification vary across flag states and operators. IMO+1
- **Limited bandwidth and intermittent connectivity,** complicating patching and remote monitoring.
- **Insecure satellite and radio links.**
- **Poor identity and access management** practices (shared passwords, no MFA).
- **Inadequate incident response capabilities** and lack of regular drills.

3. Literature Review & Industry Context

Research and industry reporting over the past decade highlight an accelerating frequency and sophistication of maritime cyber incidents:

- **Regulatory & guidance frameworks:** IMO's MSC.428(98) introduced mandatory cyber risk management within SMS. Industry bodies (ICS, BIMCO, Class Societies) and flag administrations have issued complementary guidance to operationalize these requirements. IMO+1
- **Incident analyses & trend data:** Major incidents — notably the NotPetya/Maersk disruption (2017) — demonstrated how cyber events can paralyze operations across global shipping networks and ports.

Subsequent surveys (e.g., ICS Maritime Barometer) indicate cyber risk climbing toward the top of executives' concerns, and sector guidance has proliferated (2020–2024). investor.maersk.com+1

- **Navigation system vulnerabilities:** GNSS jamming/spoofing and AIS manipulation are well-documented threats that directly affect navigational safety and maritime situational awareness; multiple case studies and academic analyses confirm practical exploits and operational impacts. MDPI+1

Collectively, literature converges on two conclusions: (1) maritime systems were not originally designed with cybersecurity in mind; and (2) layered, practical controls that integrate cyber risk into traditional safety regimes are required.

4. Methodology

This paper uses a mixed method approach: (1) systematic literature and guidance review (IMO, BIMCO, ICS, class societies, peer-reviewed studies), (2) incident case-study analysis (NotPetya/Maersk, documented AIS/GNSS spoofing events), and (3) synthesis of best practices and standards to derive an implementable resilience framework. The goal is applied: to produce actionable controls and governance recommendations suitable for ship operators, ports, and regulators.

Threat Landscape — Types & Mechanisms

i) Malware & Ransomware

Ransomware and destructive malware can spread quickly across connected corporate and operational networks; industry examples show outages of booking, terminal, and operational systems causing days of disruption and millions in losses. The NotPetya attack on Maersk in June 2017 is a paradigm: lateral propagation from IT systems disrupted critical operational services across global terminals. investor.maersk.com+1

ii) GNSS (GPS) Jamming & Spoofing

GNSS signals are weak and unencrypted in many civil systems. Both jamming (signal denial) and spoofing (false signals) can mislead navigation systems, causing position errors or false position reporting. Incidents of systematic GNSS anomalies have been reported in conflict zones and near strategic locations, with quantifiable impacts on commercial navigation. WIRED+1

iii) AIS Manipulation & Spoofing

AIS was designed for safety and tracking, not authentication. Researchers have demonstrated AIS spoofing — falsifying ship identities or positions — which can create false traffic, mask vessels, or deceive port authorities. A documented spoofing case near Elba (Dec 2019) illustrates how AIS data can be manipulated to distort maritime situational awareness. MDPI

iv) Supply-chain & Third-party Risk

Shipping increasingly relies on third-party vendors (software providers, remote engineering services, shore-side connectivity). Compromise of a supplier can become a vector for widespread disruption, as found in multiple ransomware campaigns across industries. cybereason.com

v) Human & Insider Risks

Crew phishing, misconfigured systems, poor patching, and weak access controls remain prominent causes of breaches. Training, privileged access management and insider threat controls are therefore necessary for mitigation.

5. Case Studies

5.1 NotPetya & Maersk (June 2017)

NotPetya (often attributed to state-linked activity targeting Ukraine) had a global collateral impact. Maersk experienced full outages of critical IT systems — booking, terminal operations, and internal communications — forcing manual processes, port delays and estimated losses in the hundreds of millions. The incident crystallized the sector's vulnerability to software-supply and lateral-propagation risks and catalyzed regulatory and industry action. investor.maersk.com+1

Lessons learned: supply-chain risk is real; segregation of networks and offline disaster recovery are essential; cyber incidents can become safety incidents when they disrupt operations.

5.2 GPS Spoofing Incidents (Black Sea, 2017 and later)

Several vessels in the Black Sea reported anomalous GNSS positions in 2017, with receivers indicating locations well inland — including airports. Investigations suggested deliberate spoofing in the region during that period. More recently, GNSS interference has been reported in the Baltic and other sea areas, with some states attributing disruptions to attempts to mask vessel movements or protect critical maritime assets.

Lessons learned: Navigation systems must not be treated as infallible; redundancy, cross-checks with inertial systems, and procedural mitigations are needed.

5.3 AIS/GNSS Spoofing Events (2019–2024)

Multiple documented events show ships reporting implausible positions, or entire regions experiencing GNSS anomalies. Studies and case-analyses have demonstrated spoofed AIS feeds generating false vessel tracks and GNSS spoofing affecting commercial ship navigation. These incidents highlight the real-world danger of unauthenticated navigation/identification protocols. MDPI+1

5.4 Ransomware on Ferry Operators & Ports (Selected incidents 2020–2023)

Smaller ferry operators and port service providers have been victims of ransomware, causing service disruption and travel delays. These attacks illustrate that both large and small operators must invest proportionally in cyber resilience. Axios+1

5.5 COSCO Shipping (July 2018)

COSCO's American networks experienced cyber disruption in 2018 that impacted email and internal communications. While the attack did not result in a prolonged port outage, it highlighted how carrier operations and customer-facing services can be affected even when core ship operations remain intact.

6. Findings — What Works & Where Gaps Remain

From analysis of guidance and incidents:

1. **Regulatory mandates (IMO) improved awareness and baseline adoption**, but practical implementation varies by company size, flag state oversight, and resource constraints. IMO
2. **Network segmentation and robust backup/restore practices materially reduce impact** of malware outbreaks; companies that had strong segmentation fared better in incidents. investor.maersk.com
3. **Navigation-layer threats require signal-level and operational mitigations** (detection, cross-checking sensors, operator procedures) because protocol changes to AIS/GNSS are long-term and complex. MDPI+1
4. **Awareness and training are low-cost high-impact interventions**: phishing-resistant behaviours and drill readiness reduce attack surface and improve response. ics-shipping.org

7. Recommendations — A Practical Digital Resilience Framework

I propose a layered framework combining technical, organizational and policy measures. This framework maps to IMO requirements and industry guidance and is practical for vessel operators, ports, and regulators.

7.1 Technical Controls (Engineering & Architecture)

- **Network segmentation (IT/OT isolation):** enforce unidirectional gateways where feasible; restrict remote access with jump servers, multi-factor authentication (MFA), and strong logging. (Immediate priority). ics-shipping.org
- **Endpoint hardening & patch management:** standardized baseline configurations, whitelisting for critical OT systems, scheduled secure patching windows with compensating controls for legacy gear.
- **Robust backup & rapid recovery:** offline immutable backups and tested restoration playbooks reduce ransomware impact. investor.maersk.com
- **Signal & sensor cross-checking:** integrate multiple navigation references (inertial, radar, visual fixes) and implement GNSS anomaly detection / integrity monitoring. Treat AIS as untrusted for decision-critical contexts unless corroborated. MDPI+1
- **Secure remote service management:** vet third-party remote access, require vendor security attestations, and use ephemeral privileged access.
- **Logging, monitoring & threat detection:** centralize logs, implement anomaly detection for traffic and sensor data, and subscribe to sector information-sharing feeds.

7.2 Organizational & Human Measures

- **Embed cyber risk in SMS:** update documented procedures, define roles for cyber incident commander, and formalize cyber drills that include ship-shore coordination.
- **Training & exercises:** mandatory crew training (phishing, access controls) plus table top and live cyber drills with port partners. ics-shipping.org
- **Third-party risk governance:** contractual cyber requirements for vendors, regular audits, and continuous monitoring.

- **Incident response & crisis communications:** playbooks for isolating infected segments, fall back manual procedures for navigation/communication, and clear lines to flag/port authorities.

7.3 Policy & Sector Collaboration

- **Mandatory reporting & information sharing:** creating or strengthening national/ regional reporting mechanisms and participating in sector ISACs increases situational awareness.
- **Standards & certification:** adopt class-society and flag-state aligned certification regimes for cyber risk management and introduce periodic verification audits (technical and procedural). irclass.org
- **Investment incentives:** small operators often lack resources; consider subsidies, shared security services, or port-facilitated cybersecurity clubs to pool expertise.

7.4. A Practical Cyber Risk Management Framework for Maritime Operators

This section outlines a layered but pragmatic framework operators can implement, aligned with identify–protect–detect–respond–recover principles.

7.4.1 Identify

- Asset inventory for shipboard and shore systems (hardware, software, communication links).
- Threat and vulnerability assessments considering route, cargo type, and regional geopolitical context.

7.4.2 Protect

- Network segmentation and strong boundary controls between IT and OT.
- Robust patch-management processes and secure configuration baselines.
- Identity and access management with MFA and role-based access control.
- Secure satellite and radio communications, encryption where feasible.
- Supply-chain security: vetting vendors, code-signing, and strict update procedures.

7.4.3 Detect

- Continuous monitoring where bandwidth allows; scheduled health checks and integrity checks for critical systems.
- Use of anomaly detection tools tuned for OT behaviors.

7.4.4 Respond

- Shipboard and shore incident response playbooks with clear roles and escalation paths.
- Decision matrices for navigating ransom demands, safety impacts, and regulatory notification requirements.
- Communication plans for crew, ports, customers, and regulators.

7.4.5 Recover

- Regular backups stored offline and offsite.
- Disaster recovery (DR) playbooks enabling manual operations for navigation and cargo handling until systems are restored.
- Post-incident review and lessons-learned cycles.

7.5. Technical and Operational Controls (Detailed Recommendations)

7.5.1 Shipboard Controls

- Enforce least privilege and privilege separation for crew systems and navigation equipment.
- Maintain a hardened, minimal software stack for bridge systems; remove unnecessary services.
- Implement loc

Implementation Roadmap (Tiered by Maturity)

Phase 0 — Assess & Govern (0–3 months)

- Conduct a cyber risk assessment mapped to ICS/NIST or class guidance; appoint a cyber lead and integrate cyber into SMS. ics-shipping.org

Phase 1 — Immediate Technical Hygiene (3–9 months)

- Implement segmentation, MFA for shore access, patch critical systems, and create immutable backups. Run phishing campaigns and baseline training.

Phase 2 — Detection & Response (9–18 months)

- Deploy logging/monitoring, threat intelligence feeds, and incident playbook testing including ship-shore drills.

Phase 3 — Resilience & Verification (18–36 months)

- Pursue certification where available, vendor assurance programs, and continuous improvement cycles including exercises and audits.

7.6 Limitations & Research Gaps

- **Attribution & data scarcity:** public disclosure of maritime incidents is incomplete, complicating statistical trend analysis.
- **Rapid technology change:** emerging autonomous and satellite-based services may shift threat models quickly; continuous research is required.
- **GNSS & AIS protocol evolution:** long-term mitigation may need cryptographic designs or new standards — raising technical and interoperability challenges.

8. Conclusion

Maritime cyber threats pose operational, safety and economic risks that can cascade across global supply chains. The sector has made progress — IMO requirements and industry guidelines are important milestones — but high-impact incidents and persistent vulnerabilities show that considerable work remains.

Digital resilience requires a layered approach combining technical controls (segmentation, backups, sensor cross-checks), organizational measures (SMS integration, training, vendor governance), and sector-level collaboration (reporting, standards, capacity support for small operators).

When implemented pragmatically, these measures preserve navigational safety, protect the environment, and sustain global trade in a digitized maritime era.

Hence, Maritime cybersecurity is no longer optional — it is integral to safety and efficiency at sea. Building digital resilience ensures not just protection, but operational sustainability in an interconnected maritime ecosystem.

9. References (selected, load-bearing sources)

1. IMO. **Resolution MSC.428(98) — Maritime Cyber Risk Management in Safety Management Systems** (adopted 16 June 2017). IMO
2. A.P. Møller - Mærsk A/S. **Cyber attack update (NotPetya / June 2017)**. Company press release and post-incident summaries. investor.maersk.com+1
3. Androjna, A., "AIS Data Vulnerability Indicated by a Spoofing Case-Study," *Applied Sciences*, 2021. (AIS spoofing case near Elba). MDPI

4. ICS. **ICS Maritime Barometer Report 2023–2024** (sector risk perceptions and trends). ics-shipping.org
5. BIMCO. **Guidelines on Cyber Security On board Ships** (2021). bimco.org
6. Indian Register of Shipping / Class society guidance: **Guidelines on Maritime Cyber Safety, Rev 1 (2024)** (example of class society technical guidance). irclass.org
7. Maritime Global Security. **Jamming and Spoofing of GNSS — Mitigation Practices** (industry report).