

A Systematic Literature Review of Cybersecurity Risks in Autonomous and Digitalised Maritime Systems

Achema Iyamadi Timothy; A. A. Obiniyi; and J. B. Agbogun

Federal University Lokoja, Nigeria.

Corresponding author: sarrytims1@gmail.com

DOI: <https://doi.org/10.62154/ajmbr.2026.022.01021>

Abstract

The maritime industry is experiencing rapid digitalisation driven by the adoption of autonomous vessels, cyber-physical systems, artificial intelligence, Internet of Things (IoT) technologies, and extensive ship-shore connectivity. While these developments enhance operational efficiency, safety, and sustainability, they have simultaneously expanded the cyber-attack surface of maritime systems. This study synthesises contemporary research on cybersecurity risks in autonomous and digitalised maritime environments. Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines, 52 peer-reviewed studies published between 2018 and 2025 were analysed from Scopus, Web of Science, IEEE Xplore, ScienceDirect, and ResearchGate. The review categorises the literature into three dominant themes: (i) cybersecurity risk assessment and management frameworks, (ii) vulnerabilities and threat vectors in maritime cyber-physical systems, and (iii) human, regulatory, and validation challenges. Findings reveal increasing reliance on hybrid risk assessment models integrating safety analysis techniques with cybersecurity taxonomies such as Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK), alongside emerging AI-driven approaches. However, persistent gaps remain in real-world validation, regulatory harmonisation, and human-factor integration. The study concludes that resilient autonomous maritime operations depend on empirically grounded, human-centred, and standardised cybersecurity frameworks. It further recommends future research focusing on real-world validation, regulatory harmonisation, and maritime-specific cybersecurity training.

Keywords: Maritime Cybersecurity; Autonomous Ships; Cyber-Physical Systems; Risk Assessment; Systematic Literature Review.

Introduction

The maritime industry is the backbone of global trade, accounting for over 80% of international goods transportation (United Nations Conference on Trade and Development [UNCTAD], 2023). In recent years, the sector has experienced accelerated digitalisation through the adoption of cyber-physical systems, autonomous vessels, integrated navigation platforms, satellite communication systems, and port automation technologies. While these innovations enhance efficiency, safety, and sustainability, they simultaneously expand the cyber-attack surface of maritime infrastructure, making ships (vessels), ports, and logistics chains increasingly vulnerable to sophisticated cyber threats (Martínez et al., 2024; Alvarez et al., 2023).

Critical maritime systems such as the Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS), Ballast Water Management System (BWMS), Voyage Data Recorders (VDRs), and port terminal operating systems are now interconnected with enterprise IT networks and external communication channels. This connectivity exposes maritime cyber–physical systems to malware infections, spoofing attacks, ransomware, false data injection, and advanced persistent threats (Jo et al., 2022; Söner et al., 2023). Autonomous and remotely operated vessels further intensify these risks due to their reliance on continuous ship-to-shore communication and AI-driven decision-making (Yoo and Jo, 2023).

Despite growing academic and industrial attention, maritime cybersecurity research remains fragmented across technical, human, and regulatory domains. Many proposed cybersecurity frameworks lack empirical validation, while international regulations struggle to keep pace with technological change (Karim, 2022). Although scholarly attention to maritime cybersecurity has increased, existing studies are fragmented across technical, organisational, and regulatory domains. Many proposed frameworks remain conceptual or simulation-based, with limited empirical validation in operational maritime environments (Kharchenko et al., 2022). Consequently, a systematic synthesis of existing research is essential to consolidate knowledge, evaluate methodological strengths and limitations, and identify research gaps.

This Systematic Literature Review (SLR) addresses the following research questions:

- a. How have researchers approached the assessment and management of cybersecurity risks in maritime systems?
- b. Which maritime technologies and infrastructures are most exposed to cyber threats and vulnerabilities?
- c. What major challenges and research gaps remain in achieving effective cybersecurity for autonomous and digitalised maritime operations?

The research questions presented in this section provide a broad conceptual direction for the study, while more detailed operational formulations are provided in the methodology section to guide the systematic review process.

Problem Statement

Despite the growing body of research on maritime cybersecurity, existing studies remain fragmented across technical, human, and regulatory domains. Many proposed frameworks lack empirical validation in real-world maritime environments, while issues such as inconsistent regulatory implementation and insufficient cybersecurity training continue to undermine system resilience. Furthermore, the rapid integration of emerging technologies such as artificial intelligence, Internet of Things (IoT), and digital twin systems has expanded the cyber threat landscape without corresponding advancements in comprehensive risk management strategies. This gap highlights the need for a systematic

synthesis of current research to identify key vulnerabilities, evaluate existing approaches, and provide direction for future studies.

Methodology

Research Design

This review is in accordance with the PRISMA 2020 guidelines (Page et al., 2021; Kitchenham and Charters, 2007) to ensure methodological transparency and reproducibility. Five major academic databases: Scopus, Web of Science, IEEE Xplore, ScienceDirect, and ResearchGate, were systematically searched for studies published between 2018 and 2025, reflecting the most recent developments in maritime digitalisation and cybersecurity. The process involved four main stages: (i) planning the review, (ii) conducting the search, (iii) screening and selection, and (iv) data extraction and synthesis. Although no formal theoretical framework was adopted, the PRISMA 2020 protocol and thematic synthesis approach collectively provide the methodological foundation for this study.

Research Questions

The research questions presented in this section operationalise the broader conceptual questions introduced in the Introduction, ensuring consistency between the study objectives and the systematic review process.

The formulation of research questions serves as the foundation for guiding this systematic literature review. Given the increasing digitalization of maritime operations, it is crucial to identify how existing studies have approached cybersecurity within this evolving ecosystem. The research questions were designed to explore three core dimensions of maritime cybersecurity: (i) the frameworks, models, and methodologies developed to assess and mitigate risks; (ii) the vulnerabilities, threats, and attack vectors affecting maritime systems; and (iii) the gaps that persist in human, regulatory, and validation domains. These questions aim to provide a comprehensive understanding of current advancements, limitations, and future directions for achieving a resilient maritime cyber infrastructure.

- a. What frameworks, models, and methodologies have been utilized for cyber security risks assessment and management in the maritime sector, and how well have they performed?
- b. What cyber vulnerabilities, threats, and attack vectors have been identified in maritime systems?
- c. What are the gaps in maritime cyber security regarding human factors, regulatory frameworks, and real-world validation from previous studies?

Data Sources and Search Strategy

A comprehensive search was conducted across five major academic databases: Scopus, Web of Science, IEEE Xplore, ScienceDirect, and ResearchGate. The search targeted peer-

reviewed journal articles, conference proceedings, and technical reports published between 2018 and 2025, reflecting the most relevant period of maritime digitalisation and cybersecurity evolution. The lower boundary year (2018) was treated as inclusive, ensuring that foundational studies at the early stage of maritime digitalisation were captured.

Search strings combined maritime-specific and cybersecurity-focused keywords using Boolean operators, including: ("maritime cybersecurity" OR "ship cybersecurity" OR "autonomous ships" OR "port cyber risk") AND ("risk assessment" OR "framework" OR "threat analysis" OR "vulnerability"). Only English-language studies directly related to maritime or port cybersecurity were considered.

The screening process yielded 312 records, of which 52 studies met all inclusion criteria after duplicate removal, abstract screening, and full-text eligibility assessment as illustrated in Figure 1 (PRISMA 2020 flow diagram).

Quality appraisal was conducted using the Joanna Briggs Institute (JBI) checklist, with only studies scoring above 70% retained. Data extraction focused on research objectives, methodologies, key findings, and reported limitations. A thematic synthesis approach was used to integrate qualitative and quantitative findings.

Inclusion, Exclusion, and Screening Process

The initial search yielded 312 records. After removing duplicates and applying title, abstract, and full-text screening, 52 studies met all inclusion criteria and were retained for final synthesis.

The included studies met the following criteria:

- a. Peer-reviewed journal articles, conference papers, and technical reports
- b. Focus on maritime or port cybersecurity
- c. Proposed frameworks, models, empirical analyses, or structured assessments
- d. Published in English between 2018 and 2025

Excluded studies comprised opinion pieces, non-maritime cybersecurity research, editorials, and articles lacking methodological rigor.

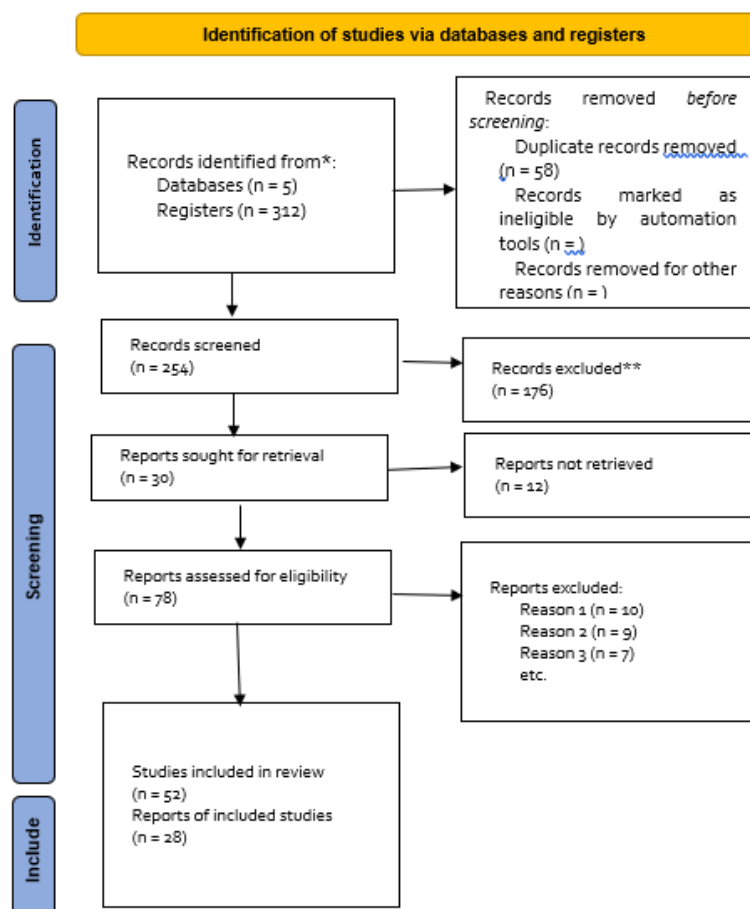


Figure 1. PRISMA flow diagram of study identification and selection

This figure illustrates the four-stage PRISMA process: identification (312 records), screening (264), eligibility (78), and final inclusion (52 studies). (Page et al., 2021)

Quality assessment was performed using the Joanna Briggs Institute (JBI) critical appraisal checklist. Only studies scoring above 70% in relevance, methodological rigor, and clarity were included.

Study Selection and Quality Assessment

From an initial 312 records, 52 studies satisfied all inclusion criteria after duplicate removal, title/abstract screening, and full-text evaluation. Methodological quality was assessed using the Joanna Briggs Institute (JBI) checklist, and only studies scoring above 70% were retained.

Data Extraction and Synthesis

A standardized data extraction form was used to collect information such as author, publication year, research objective, methodology, key findings, and identified gaps. Data extraction was conducted by a single reviewer, and consistency was ensured through repeated verification of extracted variables to minimise bias. Data synthesis combined

qualitative thematic analysis and quantitative mapping, allowing identification of research patterns and distribution across thematic categories. Descriptive statistics (e.g., frequency distribution) were used to summarize the research focus areas, while thematic synthesis highlighted emerging trends in frameworks, vulnerabilities, and policy issues.

Ethical Considerations

As this study relied solely on secondary data from published academic sources, no ethical approval was required. Nevertheless, all works were properly cited to maintain academic integrity and avoid plagiarism.

Thematic Synthesis of Findings

Maritime Cybersecurity Risk Assessment Frameworks (RQ1)

RQ1. *What frameworks, models, and methodologies have been utilized for cyber security risks assessment and management in the maritime sector, and how well have they performed?*

Table1: Distribution of Research Focus Across Frameworks, Threats, and Gaps Authors' synthesis of reviewed studies (2018–2025)

Focus Area	% of Studies Reviewed
Risk Assessment Frameworks & Models	38%
Vulnerabilities & Attack Surfaces	42%
Human/Regulatory/Validation Gaps	20%

The percentage distributions were calculated based on the frequency of studies classified under each thematic category out of the total 52 included studies.

The table 1 shows that the reviewed studies reveal that maritime cybersecurity has increasingly adopted structured risk assessment frameworks, AI-driven models, and hybrid methodologies to address threats in cyber–physical systems, vessels, and port infrastructures.

A dominant body of literature focuses on the development of structured cybersecurity risk assessment frameworks tailored to maritime cyber–physical systems. Approximately 38% of reviewed studies propose hybrid frameworks combining traditional safety analysis techniques—such as Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects, and Criticality Analysis (FMECA) with cybersecurity taxonomies like MITRE ATT&CK and MITRE D3FEND (Detect, Deny, and Disrupt Framework Empowering Network Defense) (Yousaf & Zhou, 2024; Park et al., 2023). These approaches enable systematic mapping of adversarial tactics to vulnerabilities and mitigation strategies, improving explainability and traceability.

Other studies introduced domain-specific models, such as the Cyber Risk Assessment for Ships (CRASH) methodology, which prioritises usability for maritime professionals without advanced cybersecurity expertise (Oruc et al., 2024). Probabilistic and Bayesian models

have also been proposed to quantify cyber risk likelihoods and consequences in shipboard systems (Melnyk et al., 2023). Despite their analytical sophistication, most frameworks remain validated primarily through simulations or expert judgment rather than operational deployment.

However, the literature consistently reports limited real-world deployment of these frameworks. Most validations rely on simulations, expert judgment, or hypothetical scenarios, reducing operational credibility (Kharchenko et al., 2022).

Figure 2 presents a taxonomy of cybersecurity risk assessment frameworks identified in the reviewed literature on maritime cyber-physical systems. The taxonomy categorizes the approaches used in existing studies into five major classes: traditional safety-based models, probabilistic risk models, hybrid safety-cybersecurity models, artificial intelligence (AI)-driven models, and regulatory-based frameworks. These categories reflect the evolution of cybersecurity risk assessment methodologies in the maritime sector as the industry transitions toward digitalised and autonomous ship operations.



Figure 2. Taxonomy of maritime cybersecurity frameworks identified in the literature

Hybrid risk models, probabilistic models, AI-driven approaches, and regulatory-based frameworks (Kavallieratos et al., 2019)

The first category, traditional safety-based models, includes techniques such as Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects, and Criticality Analysis (FMECA). These methods originate from reliability engineering and have been widely applied in maritime safety assessments to identify potential system failures and evaluate their consequences. In cybersecurity research, these models are adapted to analyze vulnerabilities within shipboard operational technologies such as navigation systems, propulsion control systems, and communication networks. Although effective in identifying system failures, these approaches were originally designed for safety rather than cybersecurity threats, limiting their ability to model complex cyberattack scenarios (Kavallieratos, Katsikas, & Gkioulos, 2019).

The second category comprises probabilistic risk assessment models, which include Bayesian networks, Monte Carlo simulations, and statistical risk models. These approaches quantify cyber risks by estimating the probability of attack occurrence and the potential impact on maritime operations. Probabilistic models are particularly useful for analyzing uncertainties and dynamic interactions between multiple system components. For example, Bayesian models can estimate the likelihood of cyber intrusion affecting critical maritime systems such as the Electronic Chart Display and Information System (ECDIS) or

the Automatic Identification System (AIS). However, these models often require large datasets and expert knowledge to accurately estimate probability distributions, which may limit their practical deployment in real-world maritime environments (Melnik et al., 2023). The third category represents hybrid cybersecurity frameworks, which combine traditional safety analysis techniques with modern cybersecurity intelligence frameworks. These approaches integrate safety methodologies such as FMEA with cyber threat intelligence frameworks such as MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) and MITRE D3FEND (Detect, Deny, and Disrupt Framework Empowering Network Defense). Hybrid frameworks enable researchers to systematically map cyberattack tactics to vulnerabilities and defensive strategies, thereby improving the traceability and explainability of cybersecurity risk assessments. This approach has gained significant attention in maritime cybersecurity research because it bridges the gap between engineering safety analysis and modern cyber threat modeling (Yousaf & Zhou, 2024).

The fourth category consists of AI-driven cybersecurity models, which utilize machine learning, deep learning, and data-driven analytics to detect and predict cyber threats in maritime environments. AI-based approaches are increasingly being applied to anomaly detection in AIS traffic data, intrusion detection in shipboard networks, and predictive analysis of cyber incidents. These models offer the advantage of automatically identifying patterns and abnormal behaviors within large volumes of maritime data. However, AI models may introduce additional risks such as adversarial attacks or biased predictions, and their effectiveness depends heavily on the availability of reliable training datasets (Elsisi et al., 2024).

The final category includes regulatory and standards-based frameworks, which are derived from international cybersecurity guidelines and maritime governance mechanisms. These frameworks rely on policy-driven approaches to cybersecurity risk management and include standards such as the International Maritime Organization (IMO) Guidelines on Maritime Cyber Risk Management, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and industry guidance from the Baltic and International Maritime Council (BIMCO). Regulatory frameworks emphasize compliance, governance structures, and organizational cybersecurity practices rather than technical risk modeling. They play a critical role in establishing baseline cybersecurity requirements for shipping companies, port operators, and maritime authorities (Karim, 2022).

Figure 2 illustrates the progressive evolution of maritime cybersecurity research from traditional engineering safety models toward integrated, hybrid, and AI-driven risk assessment frameworks. While traditional methods provide structured failure analysis, emerging hybrid and AI-based models offer more comprehensive capabilities for detecting and mitigating cyber threats in complex maritime cyber-physical systems. Nevertheless, the literature indicates that many of these frameworks remain conceptual or simulation-based, highlighting the need for empirical validation using real-world maritime operational data.

Despite the advances in cybersecurity frameworks, the literature reveals notable contradictions. While AI-driven models demonstrate superior predictive capabilities, several studies highlight their vulnerability to adversarial attacks and dependency on high-quality datasets. Similarly, hybrid frameworks improve analytical depth but often increase computational complexity and reduce usability for maritime practitioners. These conflicting findings suggest that no single approach fully addresses the multidimensional nature of maritime cybersecurity risks, thereby necessitating integrated and empirically validated solutions.

Vulnerabilities and Threat Vectors in Maritime Systems (RQ2)

The literature consistently identifies navigation and communication systems as primary attack targets. AIS and ECDIS vulnerabilities are extensively documented, particularly due to their lack of authentication, encryption, and intrusion detection mechanisms (Nguyen et al., 2022; Omojowo, 2026; Kayışoğlu et al., 2024). Studies demonstrate that AIS spoofing, denial-of-service attacks, and false data injection can severely compromise situational awareness and navigational safety.

Emerging research highlights advanced threats targeting AI-enabled maritime systems. Omojowo et al. (2025) demonstrate how generative adversarial networks can manipulate radar imagery, while Elsis et al. (2024) show the risks of false data injection in IoT-based maritime monitoring systems. Autonomous ships are particularly vulnerable due to continuous ship-to-shore connectivity, which increases exposure to remote cyber intrusions (Yoo & Jo, 2023).

Table 2: Commonly Reported Maritime Vulnerabilities (Kessler, 2018)

Maritime System	Key Vulnerabilities	Representative Studies
AIS (Automatic Identification System)	Spoofing, Jamming, Manipulation	Kessler (2018), Goudossis et al., (2019)
ECDIS (Electronic Chart Display & Info System)	Malware Injection, Human Error	Svilicic et al.,(2019), Tam & Jones (2019)
VDR & GMDSS	Data Manipulation, Insider Threats	Bauk (2025), Bauk (2025)
BWMS (Ballast Water Mgmt System)	Network Exploits, Weak Authentication	Zhang et al., (2022)
Port Systems	Ransomware, Supply Chain Attacks	Loomis et al., (2021), Zhang et al., (2022)

Autonomous vessels further expand the attack surface through continuous ship–shore communication and cloud-based control architectures (Yoo and Jo, 2023). Studies also show that cyberattacks often originate from enterprise IT systems before propagating to operational technology (OT) onboard ships, underscoring the need for integrated IT–OT security strategies (Kavallieratos et al., 2019).

The literature identifies several critical vulnerabilities and threats across maritime systems and infrastructures as listed in Table 2. AIS is highly exposed to spoofing, jamming, and manipulation (Kessler, 2018; Goudossis et al., 2019). ECDIS is vulnerable to malware injection and operator error, highlighting both technical and human factors (Svilicic et al., 2019; Tam & Jones, 2019). VDR and GMDSS systems face risks of data manipulation and insider threats (Bauk, 2025). BWMS suffers from network exploits and weak authentication, creating entry points for cyberattacks (Zhang et al., 2022). Finally, port systems are increasingly targeted by ransomware and supply chain attacks, posing systemic risks to global trade (Loomis et al., 2021; Zhang et al., 2022). Collectively, these findings show that maritime attack surfaces span onboard vessel systems, operational technologies, and interconnected port infrastructures

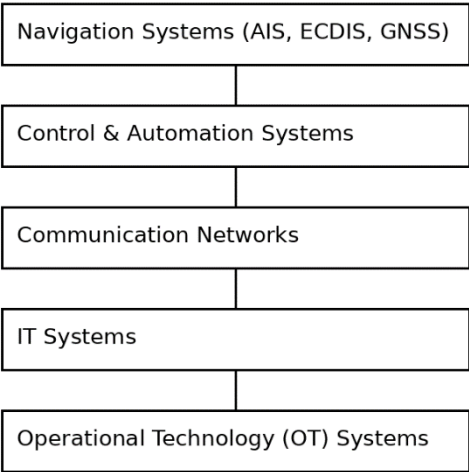


Figure 3. Identified gaps in maritime cybersecurity research
Technical validation gaps, human-factor vulnerabilities, and regulatory inconsistencies (Karim, 2022)

Human and Regulatory Dimensions of Maritime Cybersecurity (RQ3)

Beyond technical vulnerabilities, human factors and regulatory deficiencies remain critical weaknesses in maritime cybersecurity. Empirical studies demonstrate low levels of cybersecurity awareness among seafarers and maritime students, increasing susceptibility to phishing, insider threats, and misconfigurations (Karaca & Söner, 2023; Kayisoglu et al., 2022). Although training frameworks have been proposed, standardized cybersecurity education under the International Convention on Standards of Training, Certification, and Watchkeeping (STCW) is still lacking.

Table3: Remaining Maritime Cybersecurity Gaps (Authors' synthesis based on Karim (2022), Kavallieratos et al. (2019)).

Gap Category	Description	% of Studies Highlighting Gap
Human Factors	Lack of seafarer training & awareness	35%
Regulatory	Weak enforcement & inconsistent standards	28%
Validation	Lack of real-world testbeds & empirical studies	37%

From Table 3, the reviewed studies propose multiple frameworks and defense mechanisms to strengthen maritime cybersecurity. Regulatory and standards-based frameworks such as the IMO MSC-FAL.1/Circ.3 (International Maritime Organisation Maritime Safety Committee – Facilitation Committee Circular 3) guidelines, NIST (National Institute of Standards and Technology) Cybersecurity Framework, and BIMCO's (Baltic and International Maritime Council) guidelines are widely referenced for establishing baseline security practices (Loomis et al., 2021; Tam & Jones, 2019). Technical defense mechanisms include intrusion detection systems tailored to maritime traffic (Kessler, 2018), anomaly detection models for AIS data (Goudossis et al., 2019), and secure authentication protocols for shipboard networks (Zhang et al., 2022). Organizational measures emphasize crew training, incident response planning, and cyber risk assessments, addressing the human factor as a persistent vulnerability (Svilicic et al., 2019; Bauk, 2025). Best practices also include network segmentation, regular patching, and penetration testing to reduce attack surfaces in port and vessel systems (Bauk, 2025; Zhang et al., 2022). Collectively, these frameworks and mechanisms converge on a defense-in-depth strategy, integrating regulatory compliance, technical safeguards, and human-centered practices to enhance resilience of critical maritime infrastructures.

Regulatory analyses further indicate that existing International Maritime Organization (IMO) guidelines are insufficiently enforced and inconsistently adopted across regions, particularly in developing economies (Karim, 2022; Karim, 2022). Moreover, many proposed cybersecurity frameworks lack empirical validation using real-world maritime datasets, underscoring a significant research-to-practice gap (Kharchenko et al., 2022).

Discussion

The systematic review reveals that maritime cybersecurity research has evolved from descriptive risk assessments toward more structured, hybrid, and AI-assisted frameworks. Approximately 38% of studies focused on risk assessment frameworks and models, underscoring the growing emphasis on systematic evaluation and quantification of cyber risks. Frameworks such as FMECA-ATT&CK (Kavallieratos et al., 2019) and Cyber Risk Assessment for Ships (CRASH) (Oruc et al., 2024) illustrate a methodological shift toward integrating engineering reliability analysis with cybersecurity taxonomies like MITRE ATT&CK and NIST. This hybridization reflects the sector's recognition that maritime

systems, particularly autonomous and cyber-physical infrastructures require multidimensional approaches that combine safety, reliability, and information security.

However, the analysis also indicates a divergence between theoretical frameworks and operational validation. While many proposed models achieve conceptual robustness, few undergo empirical testing within real maritime environments. This limitation is critical because maritime operations involve dynamic, interconnected systems that differ from static industrial networks. For instance, AI-driven risk models and simulation-based frameworks (Kharchenko et al., 2022; Elsis et al., 2024) demonstrate strong potential for proactive threat detection and system optimization but often rely on synthetic or simulated datasets, reducing their reliability in field applications.

The persistence of the validation gap can be attributed to structural constraints such as restricted access to real maritime operational data due to security concerns, high costs associated with cyber range development, and the absence of standardized testing environments. These limitations significantly hinder the transition from theoretical models to operational deployment.

In terms of threat surfaces, the review identifies AIS, ECDIS, BWMS, and port management systems as the most targeted components, aligning with global maritime security incident reports. AIS spoofing and jamming, ECDIS malware injection, and port ransomware attacks collectively highlight the convergence of cyber and operational vulnerabilities. These threats stem not only from technological weaknesses but also from inadequate human awareness, insufficient regulatory enforcement, and fragmented data governance. Indeed, the persistence of insider threats and human error (Svilicic et al., 2019; Bauk, 2025) underscores that cybersecurity in the maritime domain is as much a human challenge as it is a technical one.

The reliance on simulated environments rather than real-world deployments is further reinforced by the use of cybersecurity testbeds, which, although effective for controlled experimentation, may not fully capture operational complexities (Kavallieratos et al., 2019). Regulatory and policy challenges remain a persistent weakness in maritime cybersecurity. Although frameworks such as IMO guidelines and BIMCO recommendations provide direction, their implementation is inconsistent across jurisdictions and vessel types, as reflected in the 28% of studies identifying regulatory gaps. Similarly, human factors remain underdeveloped compared to technological defences, with 35% of studies highlighting issues related to training and cyber hygiene.

The growing adoption of AI, IoT, and digital twin technologies introduces both opportunities and risks. While these technologies enable predictive maintenance and continuous risk monitoring, they also expand the cyberattack surface and require more sophisticated security measures. However, the limited real-world validation of existing models reduces their practical applicability in maritime environments.

Addressing these challenges requires a balanced approach that integrates technological solutions with regulatory harmonisation and human capacity development. Technical

measures alone are insufficient; effective maritime cybersecurity depends on interdisciplinary collaboration, combining enforceable policies, human-centred training, and continuous monitoring systems.

Conclusion

This systematic literature review synthesised existing research on cybersecurity risks in autonomous and digitalised maritime systems, revealing significant advancements in hybrid and AI-driven risk assessment frameworks. However, critical gaps persist in empirical validation, human capacity development, and regulatory enforcement. Future research should prioritise real-world implementation of cybersecurity frameworks, development of standardized maritime cybersecurity education, and harmonisation of global regulatory policies. Addressing these challenges is essential for ensuring the secure and resilient operation of next-generation autonomous maritime systems.

Recommendations

- i. **For Researchers:** Future studies should prioritise empirical validation of cybersecurity frameworks using real-world maritime datasets and develop standardised benchmarking environments.
- ii. **For Industry Practitioners:** Maritime organisations should implement continuous cybersecurity training, adopt defence-in-depth strategies, and integrate IT–OT security frameworks.
- iii. **For Policymakers:** Regulatory bodies should enforce harmonised international cybersecurity standards and mandate compliance with frameworks such as IMO and NIST..

References

- Alvarez, C., Hinojosa, C., Gonzalez, S., & Rojas, L. (2023). Towards Cybersecure Maritime Supply Chains in Latin America and the Caribbean. In *Lecture Notes in Logistics: Vol. Part F268*. https://doi.org/10.1007/978-3-031-32032-3_19
- Bauk, S. (Ed.). (2025). *Maritime cybersecurity*. Springer. <https://doi.org/10.1007/978-3-031-87290-7>
- Elsisi, M., Yu, J. T., Lai, C. C., & Su, C. L. (2024). A Drone-Assisted Deep Learning-Based IoT System for Monitoring Ship Emissions in Ports Considering Adversarial Attacks. *IEEE Transactions on Instrumentation and Measurement*, 73. <https://doi.org/10.1109/TIM.2024.3374306>
- Goudossis, A., & Katsikas, S. K. (2019). Towards a secure Automatic Identification System (AIS). *Journal of Marine Science and Technology*, 24, 410–423. <https://doi.org/10.1007/s00773-018-0561-3>
- Jo, Y., Choi, O., You, J., Cha, Y., & Lee, D. H. (2022). Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework. *Sensors*, 22(5). <https://doi.org/10.3390/s22051860>
- Karaca, I., & Söner, Ö. (2023). An evaluation of students' cybersecurity awareness in the maritime industry. *International Journal of 3D Printing Technologies and Digital Industry*, 7(1). <https://doi.org/10.46519/ij3dptdi.1236264>
- Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*, 143. <https://doi.org/10.1016/j.marpol.2022.105138>

- Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2019). Cyber-attacks against ship systems: A systematic literature review. *Journal of Marine Science and Engineering*, 7(10), 352. <https://doi.org/10.3390/jmse7100352>
- Kayisoglu, G., Bolat, P., & Tam, K. (2022). Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime. *Journal of Navigation*, 75(6). <https://doi.org/10.1017/S0373463322000534>
- Kayısoğlu, G., Güneş, B., & Bolat, P. (2024). ECDIS Cyber Security Dynamics Analysis based on the Fuzzy FUCOM Method. *Transactions on Maritime Science*, 13(1). <https://doi.org/10.7225/toms.v13.n01.w09>
- Kessler, G. C., Craiger, J. P., & Haass, J. C. (2018). A taxonomy framework for maritime cybersecurity: A demonstration using the Automatic Identification System. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 12(3), 429–437. <https://doi.org/10.12716/1001.12.03.01>
- Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (EBSE Technical Report EBSE-2007-01). Keele University. https://www.elsevier.com/_data/promis_misc/525444systematicreviewsguide.pdf
- Loomis, W., Singh, V. V., Kessler, G. C., & Bellekens, X. (2021). A system of systems: Cooperation on maritime cybersecurity. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-a-system-of-systems>.
- Martínez, F., Sánchez, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2024). Maritime cybersecurity: protecting digital seas. *International Journal of Information Security*, 23(2). <https://doi.org/10.1007/s10207-023-00800-0>
- Melnyk, O., Onyshchenko, S., Onishchenko, O., Lohinov, O., & Ocheretna, V. (2023). Integral approach to vulnerability assessment of ship's critical equipment and systems. *Transactions on Maritime Science*, 12(1).
- Melnyk, O., Onyshchenko, S., Pavlova, N., Kravchenko, O., & Borovyk, S. (2022). Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. *IJCSNS International Journal of Computer Science and Network Security*, 22(3).
- Nguyen, D., Vadaine, R., Hajduch, G., Garelllo, R., & Fablet, R. (2019). *GeoTrackNet: Maritime anomaly detection using AIS data*
- Omojowo F. A., Edgar Osaghae, and Taiwo Kolajo. (2025). Evaluating covid-19 public discourse for sentiment, topic, and geolocation analysis. *J. Electr. Syst. Inf. Technol.*, 12(1):15.
- Omojowo F. A. (2026). Topic evolution in social media discourse during global health emergencies. *J. Electr. Syst. Inf. Technol.*, 13(1):7.
- Oruc, A., Chowdhury, N., & Gkioulos, V. (2024). A modular cyber security training programme for the maritime domain. *International Journal of Information Security*, 23, 1477–1512. <https://doi.org/10.1007/s10207-023-00799-4>.
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Svilicic, B., Brčić, D., Žuškin, S., & Kalebić, D. (2019). Raising awareness on cyber security of ECDIS. *TransNav*, 13(1), 231–236. <https://doi.org/10.12716/1001.13.01.24>
- Tam, K., & Jones, K. (2019). Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, 4(2), 147–164. <https://doi.org/10.1080/23738871.2019.1596964>
- United Nations Conference on Trade and Development. (2023). *Review of maritime transport 2023*. United Nations. <https://unctad.org/publication/review-maritime-transport-2023>

- Yoo, J., & Jo, Y. (2023). Formulating Cybersecurity Requirements for Autonomous Ships Using the SQUARE Methodology. *Sensors*, 23(11). <https://doi.org/10.3390/s23115033>
- Yousaf, A., & Zhou, J. (2024). From sinking to saving: MITRE ATT &CK and D3FEND frameworks for maritime cybersecurity. *International Journal of Information Security*, 23(3). <https://doi.org/10.1007/s10207-024-00812-4>
- Zhang, P., Wang, Y., Aujla, G. S., Jindal, A., & Al-Otaibi, Y. D. (2022). A blockchain-based authentication scheme for IoT-enabled maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*. <https://doi.org/10.1109/TITS.2022.3159485>