UMT PRESS

Journal of Maritime Logistics
Journal Homepage: https://journal.umt.edu.my/index.php/jml
e-ISSN: 2805-5195
DOI: http://doi.org/10.46754/jml.2026.08.005

THE UNSEEN STORM: A CRITICAL REVIEW OF CYBERSECURITY THREATS AND THEIR ECONOMIC IMPACT ON GLOBAL MARITIME TRADE

MUHAMMAD JAHANZAIB SULTAN*

Master of Maritime Operations and Management, UniKL MIMET, Universiti Kuala Lumpur, 32200 Lumut, Perak, Malaysia
**Corresponding author: muhammad.jahanzaib@s.unikl.edu.my*

ARTICLE INFO

Article History:
Received: 15 November 2025
Revised: 4 March 2026
Accepted: 1 April 2026
Published: 15 August 2026

Keywords:
Maritime cybersecurity, Shipping 4.0, IMO cyber risk, economic impact of cyber-attack, supply chain disruption

ABSTRACT

The maritime industry, the silent engine of global trade, is undergoing a profound digital transformation, often referred to as Shipping 4.0 (Mesa *et al*., 2024). This significant shift involves the widespread adoption of digital, interconnected operating environments known as Cyber-physical Systems. While this technological leap has brought about remarkable improvements in efficiency and competitiveness, it has also, ironically, exposed the sector to a new wave of complex cybersecurity threats. This critical review paper delves into the rapidly changing landscape of maritime cyber threats and, crucially, assesses their tangible economic impact on global maritime trade. Our investigation begins by mapping out the primary vulnerabilities found in both shipboard and port-side systems. We pay special attention to mission-critical technologies like the Electronic Chart Display and Information System (ECDIS), GNSS, and automated cargo-handling infrastructure. Key real-world incidents, such as the devastating NotPetya attack on A.P. Moller-Maersk, are analysed not only to illustrate the threat but also to provide an empirical basis for quantifying the full spectrum of costs. These costs include staggering direct financial losses, widespread trade disruption, significant reputational damage, and an inevitable rise in insurance premiums across the sector. Furthermore, the study critically reviews existing global policy and regulatory frameworks, specifically examining the effectiveness of instruments like the IMO Guidelines on Maritime Cyber Risk. This analysis highlights critical gaps in their practical implementation, particularly the persistent lack of economic incentives needed to encourage robust, industry-wide security investments. Ultimately, this paper concludes by offering strategic, economically sound recommendations designed to foster strong cyber-resilience, which is vital for protecting the integrity and efficiency of the critical maritime supply chain in this fast-evolving digital age.

Introduction

The maritime industry is unequivocally the lifeblood of the global economy, transporting over 80% of the world's trade volume by weight (Mesa *et al*., 2024). For centuries, maritime transport has been the driving force behind globalisation and intercontinental supply chains. Today, this colossal industry is navigating its fourth major technological revolution—an era defined by rapid digitalisation and extensive automation, aptly termed Shipping 4.0 or Maritime 4.0 (Bocayuva, 2021; Mesa *et al*., 2024).

This profound transformation is largely fueled by a relentless pursuit of greater operational efficiency, a competitive edge, and significantly reduced long-term operating costs. Achieving this goal requires the deep and complex integration of two previously distinct technological domains: Information

Technology systems, which typically handle business administration, documentation, and crew management; and Operational Technology systems, which directly control critical assets like propulsion, navigation, steering, and cargo handling equipment (Mesa *et al*., 2024).

However, this increased connectivity and heavy reliance on extensive, intricate Cyber-physical Systems have simultaneously created a vastly expanded and more complex attack surface (Androjna *et al*., 2020; Bocayuva, 2021). Systems on a modern vessel or within a large port facility, once physically or digitally isolated—or "air-gapped"—are now routinely and constantly connected to the public internet or external networks. This exposure makes them highly vulnerable to sophisticated and multifaceted cyber-attacks. It is crucial to understand that cyber incidents within the maritime sector are not merely minor IT issues; they represent a profound and existential threat to maritime safety, the delicate marine environment, and the essential economic viability of the entire global supply chain (Androjna *et al*., 2020).

Empirical evidence and past studies consistently show that the maritime sector operates in a high-impact, low-frequency risk environment (Afenyo & Caesar, 2023). This means that while destructive cyber-attacks may not happen daily, when they do strike, their consequences are both severe and financially devastating (Androjna *et al*., 2020). The economic ripple effects of a major maritime cyber-attack can spread far beyond the immediate target—be it an affected vessel, port terminal, or logistics provider. These consequences cascade through the global economic fabric, leading to crippling cargo delays, significant trade route disruption, massive increases in freight rates, and ultimately costing the global economy and consumers billions in damages (Afenyo & Caesar, 2023; Kechagias *et al*., 2022). Therefore, this paper emphasises the vital need to critically examine this convergence of threats and quantify the true costs associated with digital risk in the world's most critical transport artery.

Methodology

This paper utilises a Critical Review methodology to systematically assess the complex and evolving interplay of contemporary cybersecurity threats and their measurable economic impacts within the global maritime industry. The approach is fundamentally qualitative and analytical, designed to synthesise existing knowledge, pinpoint systemic gaps in current research and policy, and offer strategic, evidence-based recommendations.

Literature Search and Inclusion Criteria

The foundational data for this review was gathered through a systematic search strategy focusing exclusively on authoritative academic, governmental, and high-level industry sources.

Databases

Primary searches were conducted across established academic databases, complemented by critical reviews of major maritime industry reports (e.g., BIMCO, ICS, classification societies), regulatory body documents, and authoritative financial reports (e.g., Lloyd's, major insurance carriers).

Data Synthesis and Analytical Frameworks

The collected literature and data underwent rigorous thematic analysis, which categorised the findings into three interconnected core analytical areas.

Critical Assessment and Case Study Analysis

The final stage involved a critical assessment of the synthesised literature to identify significant policy and research gaps, which then informed the conclusions and recommendations.

Cybersecurity Threats, Vulnerabilities, and Resilience in the Maritime Domain

The maritime sector is currently on a transformative journey, commonly labelled Shipping 4.0—an inevitable evolution propelled by the aggressive integration of Information Technology and Operational Technology systems. While this modernisation drive—the

pursuit of seamless integration, automation, and data-driven decision-making—undoubtedly promises significant advantages in increased efficiency, securing a competitive edge, and facilitating autonomous operations, it simultaneously and unavoidably enlarges the sector's cyber attack surface. This expanded area introduces new and profoundly severe risks that threaten not only financial stability but also the fundamental principles of safety at sea, global security, and the reliable functioning of the global supply chain.

The International Maritime Organisation, recognising this systemic shift, has formally designated cyber risk as a critical, integrated component of a ship's Safety Management System. This landmark declaration clearly highlights a paradigm change: Cyber threats are no longer seen as mere auxiliary IT department concerns but must be managed as fundamental major safety and operational hazards. A retrospective analysis of significant maritime cyber incidents over a decade (2010 to 2020) empirically confirms a recurring pattern: These events generally occur infrequently but carry an alarmingly high potential impact, necessitating comprehensive, risk-based management strategies.

Threat Vectors in Mission-Critical Shipboard Systems

The modern cyber threat landscape is largely shaped by vulnerabilities within the crucial systems that govern a vessel's navigation, control, and overall operational stability. When these areas are compromised, what might seem like a simple technical glitch can rapidly escalate into a humanitarian or economic crisis.

Navigation and Positioning Systems

At the heart of a vessel's core operations are its navigation and manoeuvring systems, which now rely almost entirely on digital, interconnected, and globally networked components.

Global Navigation Satellite Systems/GPS

These widely used systems are now known to be highly susceptible to sophisticated spoofing attacks. During such attacks, cleverly designed false Position, Navigation, and Timing signals are deliberately sent to trick the vessel's receivers. A successful spoofing attack is far from harmless; it can directly lead to disastrous outcomes, including loss of life, collisions at sea, dangerous groundings, or a complete loss of control over the ship's movement. A notable and well-documented incident involved an $80 million superyacht that was secretly hijacked and rerouted through an expertly executed GPS spoofing manoeuvre, clearly demonstrating the seriousness of this threat.

Electronic Chart Display and Information System

Today, the Electronic Chart Display and Information System (ECDIS) is the primary and indispensable tool for electronic navigation. It is a highly complex, computer-based Operational Technology system. Significant vulnerabilities often hide within its underlying operating system or in third-party applications integrated with it. These systems can be compromised through removable media (like infected USB drives) or by connections to less secure vessel networks, thereby severely endangering safe navigation and data integrity.

Automatic Identification System

Automatic Identification System (AIS) is essential for real-time vessel tracking, identification, and collision avoidance. The main threats here involve data manipulation and spoofing, which fundamentally undermine the reliability of real-time vessel traffic information. Such calculated attacks can create "ghost" vessels on other ships' screens or strategically alter the true identity, course, and destination of specific targets.

Integrated Bridge and Ship/Shore Control Systems

The vital connection between a ship and the shore is managed by complex satellite communication and control systems. These represent significant, high-value entry points for malicious actors aiming for widespread disruption.

Operational Technology/Industrial Control Systems

These critical systems are the digital backbone of a vessel, managing propulsion, controlling power distribution networks, and coordinating complex cargo handling operations. The development of specialised assessment tools, such as the BRidge Attack Tool, has systematically revealed existing vulnerabilities within the data communication protocols of Integrated Bridge Systems. This provides undeniable proof that these physical control systems are highly vulnerable to data manipulation and operational disruption.

Satellite Communication (VSAT/Satcom)

These systems serve as the crucial, high-bandwidth link between a vessel and its shore-based management. They are chronically vulnerable to attacks designed to completely disrupt communication, facilitate covert remote sabotage of ship systems, or act as a primary, back-door route for mass malware infections across an entire fleet.

Major Threat Actors and Historical Incidents

The maritime sector currently faces a diverse range of threat actors, including financially motivated cybercriminals, strategically focused state-sponsored entities, and ideologically driven hacktivists. Each group has distinct motivations and varying levels of potential impact.

Ransomware and Systemic Supply Chain Disruption

Ransomware remains one of the most visible and financially devastating threats, especially when aimed at crucial shoreside infrastructure. The primary goal is pure financial gain achieved through forced operational disruption. The NotPetya attack on A.P. Moller-Maersk in 2017 stands as the definitive, most frequently cited global example, directly causing immense financial losses and effectively paralysing a significant portion of the global maritime supply chain for weeks.

Targeted Attacks on Ports and Critical Infrastructure

Port facilities are explicitly categorised as critical national infrastructure due to their geopolitical and economic importance, and their rapidly increasing digitalisation makes them prime targets. Documented incidents, such as a highly disruptive cyberattack on a key Iranian port facility in 2020, clearly demonstrated the potential for state-level actors to use cyber tools to target port operational systems for strategic geopolitical aims. Furthermore, ports in high-value regions like the European Union have reported a noticeable increase in complex cyberattacks, a trend that accelerated significantly after the COVID-19 pandemic and subsequent geopolitical tensions.

Cyber Risk Management and Operational Resilience

The extensive shift from older analogue systems to highly integrated digital systems has necessitated a fundamental change in the maritime industry's operational focus. This means moving from relying solely on traditional physical security to implementing comprehensive, enterprise-wide Cyber Risk Management strategies (Mraković & Vojinović, 2019; Park *et al*., 2023). This crucial section examines the regulatory forces driving this change, the common risk assessment methodologies, and the overall conceptual shift towards building lasting operational resilience against future cyber threats.

The Regulatory Imperative: IMO and Safety Management Systems

The fundamental, non-negotiable force driving formal maritime cyber risk management is the International Maritime Organisation (Mraković & Vojinović, 2019). Recognising that cyber incidents directly and profoundly threaten the core Safety Management System and the safety of human life at sea, the IMO issued Resolution MSC.428 in 2017, which was later reinforced by the clarifying MSC-FAL.1/Circ.3 (Jo *et al*., 2022; Mesa *et al*., 2024; Park *et al*., 2023).

The Mandate

This landmark resolution unequivocally stipulated that cyber risk must be appropriately and systematically addressed within a ship's existing Safety Management Systems. This was required no later than the first annual verification of the Document of Compliance after 1 January 2021 (Mraković & Vojinović, 2019; Park *et al*., 2023; Yoo & Park, 2021).

Integration Necessity

This clear regulatory mandate compelled shipowners and operators to fully integrate cyber risk assessment and mitigation into their established International Safety Management Code procedures. The goal was straightforward: to ensure that cybersecurity is treated and managed as an operational safety concern—a matter of seaworthiness—rather than being compartmentalised as a separate IT department issue (Jo *et al*., 2022; Mraković & Vojinović, 2019; Park *et al*., 2023; Yoo & Park, 2021). The IMO deliberately champions a risk-based approach, actively encouraging individual companies to identify, document, and proactively address their specific, unique vulnerabilities (Mesa *et al*., 2024).

Modern Cyber Risk Assessment Frameworks

To comply with the strict IMO mandate, and more importantly, to strategically prioritise and justify mitigation efforts, maritime stakeholders have increasingly adopted and adapted specialised risk assessment frameworks.

Failure Mode and Effects Analysis

FMEA, traditionally a core safety engineering tool, has been creatively combined with advanced techniques like Rule-based Bayesian Networks. This offers a more nuanced assessment of maritime cybersecurity risks (Park *et al*., 2023). This hybrid, systemic approach allows for a comprehensive, probabilistic evaluation of how the failure of a single component (often triggered by a cyber-attack) dynamically affects the entire ship's operation, directly addressing the complex interdependencies between IT and OT systems (Park *et al*., 2023).

NIST Cybersecurity Framework

The comprehensive National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), especially its newest version, is becoming an increasingly influential tool for structuring an organisation's overall enterprise cybersecurity program (Mraković & Vojinović, 2019). It provides a standardised, internationally recognised model for managing and systematically reducing cyber risk, built around five core, sequential functions: Identify, Protect, Detect, Respond, and Recover (Dimakopoulou & Rantos, 2024; Jo *et al*., 2022; Yoo & Park, 2021).

Specialised Maritime Tools for Assessment

Specialised tools and immersive environments are actively being developed to facilitate realistic, high-fidelity assessment and personnel training.

Cyber Ranges

These sophisticated virtual or physical environments (such as the open-source project MaCySTe) function by creating a detailed digital twin of a ship's onboard cyber-physical systems and network infrastructure (Tam *et al*., 2020). Cyber ranges allow security personnel and operators to simulate real-world cyber-attacks (e.g., GPS spoofing, network intrusions) in a totally controlled environment. This rigorously tests the effectiveness of countermeasures and provides experiential training for personnel in rapid incident response, directly linking risk assessment to practical defence capability (Afenyo & Caesar, 2023; Dimakopoulou & Rantos, 2024; Tam *et al*., 2020).

Bridge Attack Tool

As previously mentioned, BRAT is a specialised utility developed explicitly to systematically assess vulnerabilities in the data communication protocols of Integrated Bridge Systems. This demonstrates the industry's focused effort on addressing system-specific operational technology threats (Hemminghaus *et al*., 2021).

Building Operational Resilience and Mitigation Strategies

A truly resilient maritime organisation must go beyond merely implementing defences against known threats; it must actively strive to ensure operational continuity even in the face of a successful attack. Resilience, in the context of maritime operations, is therefore defined as the ability of a vessel or system to prevent, absorb the shock of, rapidly recover from, and ultimately adapt to a disruptive event, particularly a cyber-attack (Dominguez-Péry *et al*., 2023; Mesa *et al*., 2024).

Technical and Architectural Mitigation

Defence in Depth and Network Segmentation

The core technical principle here is segmentation—the strategic division of a vessel's network to isolate critical OT systems (like propulsion and navigation) from non-critical IT systems (such as crew Wi-Fi or administrative networks) (Androjna *et al*., 2020; Li *et al*., 2024; Progoulakis *et al*., 2021). This essential barrier dramatically limits lateral movement, preventing a breach in a potentially softer corporate network from escalating into a catastrophic safety-critical incident (Li *et al*., 2024).

System Hardening and Redundancy

Hardening involves implementing stringent cybersecurity baseline controls across all critical systems. For highly vulnerable navigation systems like GNSS/GPS, effective mitigation requires multi-sensor, multi-constellation receivers. Crucially, it also means actively maintaining and keeping non-GNSS-dependent backup systems (such as celestial navigation or eLoran) ready for immediate use. This provides a necessary safeguard against highly effective spoofing attacks (Androjna *et al*., 2020; Farah *et al*., 2022; Li *et al*., 2024).

Cyberattack Modelling

Sophisticated frameworks like MITRE ATT&CK are now being used to model and thoroughly understand the tactics, techniques, and procedures that potential attackers might employ (Jo *et al*., 2022). This proactive intelligence enables the creation of customised, robust detection and response plans specifically tailored to a ship's unique equipment and network architecture (Bolbot *et al*., 2022).

Organisational and Human Mitigation

The human element is consistently identified as a critical vulnerability point, yet it also represents the single most important asset in achieving resilience (Androjna *et al*., 2020; Park *et al*., 2023).

Training and Awareness

Deploying effective, continuous training programs and utilising the aforementioned cyber ranges are paramount for raising awareness among both crew and shore staff. This builds the necessary technical and non-technical skills required to manage an incident. Such training includes proper, secure procedures for handling removable media (Kechagias *et al*., 2022) and the ability to instantly recognise sophisticated social engineering attempts like spear-phishing (Ashraf *et al*., 2022; Karaś, 2023; Kechagias *et al*., 2022; Mesa *et al*., 2024).

Incident Response Planning

True operational resilience depends on having detailed, frequently tested Incident Response Plans that prioritise rapid recovery and business continuity above all else (Dimakopoulou & Rantos, 2024; Kechagias *et al*., 2022; Mraković & Vojinović, 2019). This level of operational readiness is vital for minimising the duration and economic impact of a successful attack, preventing the prolonged, paralysing effects observed in incidents like the Maersk NotPetya breach.

Economic Consequences and Policy Gaps

While the accelerating digitalisation in the maritime sector undeniably acts as a catalyst for operational efficiency and automation, it has simultaneously exposed the industry to systemic cyber risks that carry severe and often catastrophic economic consequences (Bocayuva, 2021; Farah *et al*., 2022; Kechagias

et al., 2022). A precise, granular understanding of these financial consequences is not merely an academic exercise; it is essential for formulating effective, economically viable policy and industry responses (Afenyo & Caesar, 2023).

The Direct and Systemic Costs of Maritime Cyber Incidents

The economic impact of maritime cyber threats fundamentally extends far beyond initial ransom demands or immediate IT recovery expenditures. It triggers a cascading, systemic financial damage that ripples throughout the entire global supply chain ecosystem (Androjna *et al*., 2020; Kechagias *et al*., 2022).

Direct Costs and Business Interruption

Direct financial losses immediately arise from a confluence of multiple sources.

Incident Response and Remediation

These costs cover the immediate outlay for forensic analysis, the complex effort required to restore affected systems, and the essential, yet often expensive, engagement of external cybersecurity experts (Kechagias *et al*., 2022).

Lost Revenue and Operational Downtime

This represents the quantifiable revenue loss resulting from forced port closures, severe cargo delays, and ships being compelled to operate inefficiently on manual systems or sit completely idle, effectively losing all capacity (Afenyo & Caesar, 2023; Kechagias *et al*., 2022; Park *et al*., 2023).

Reputational Damage

A highly publicised breach can trigger a profound loss of customer confidence and the termination of high-value contracts, leading to significant, often irreversible erosion of long-term market share (Afenyo & Caesar, 2023; Kechagias *et al*., 2022). The most definitive and widely cited illustration of this devastating financial impact is the 2017 NotPetya ransomware attack that targeted A.P. Moller-Maersk. This single event instantly rendered thousands of servers and critical applications inoperable across the company's massive global network. Maersk subsequently estimated the total financial damage from the incident to fall conservatively between 300 million USD, overwhelmingly due to prolonged business interruption and intensive recovery efforts (Kechagias *et al*., 2022; Park *et al*., 2023).

Systemic and Global Economic Impact

Given that roughly 90% of global trade is physically carried by sea, a successful, coordinated, systemic cyberattack on key logistical nodes could trigger a cataclysmic effect on the world economy. An attack targeting a major container terminal can rapidly cripple the logistics infrastructure supporting entire continental regions (Kechagias *et al*., 2022).

Respected experts and institutions, including authoritative reports from Lloyd's of London, have conservatively postulated that a highly successful, simultaneous attack on multiple major Asian ports could result in global losses exceeding $100 billion USD in the first year alone (Kechagias *et al*., 2022). This massive projected figure accounts for the following cost propagation.

Supply Chain Disruptions

Delays in the transport of both raw materials and finished goods rapidly cascade, halting global manufacturing processes and triggering steep spikes in consumer prices due to scarcity (Afenyo & Caesar, 2023).

Increased Insurance Premiums

A sustained, sectoral rise in premiums for cyber, cargo, and hull & machinery insurance is inevitable as risk modelling agencies recalibrate their assessments to accurately reflect the pervasive new threat landscape (Afenyo & Caesar, 2023; Kechagias *et al*., 2022).

Trade Volume Loss

The long-term impact includes trade diversion to more resilient, if less efficient, routes or an outright contraction of global trade as businesses seek greater reliability over cost efficiency.

Policy Gaps and Future Research Directions

Despite the clear, escalating, and costly economic threat, the current policy and regulatory framework suffers from significant, exploitable gaps, providing a critical area for immediate future research and legislative action (Afenyo & Caesar, 2023).

Legal and Regulatory Fragmentation

A major, persistent gap is the fundamental lack of international harmonisation in cybersecurity regulation. While IMO Resolution MSC.428 rightly mandates addressing cyber risk in Safety Management Systems, the precise technical standards and robust enforcement mechanisms are often delegated to fragmented national and flag-state legislation. This creates an environment conducive to regulatory arbitrage, where less stringent jurisdictions may be inadvertently targeted or exploited by malicious actors.

Research Gaps in Data and Economic Quantification

The ability to accurately quantify the problem is severely hampered by data deficiencies.

Data Scarcity

The true, comprehensive economic impact remains profoundly obscured by the industry's entrenched culture of non-disclosure. Companies often fear the cascading reputational and financial damage resulting from public disclosure more than they fear regulatory penalties (Afenyo & Caesar, 2023; Kechagias *et al*., 2022). This culture leads to severe underreporting of cyber incidents, making it impossible for researchers to quantify the scope of the problem fully.

Absence of Standardised Metrics

A significant gap currently exists in developing a standardised, industry-wide risk assessment methodology that seamlessly integrates both IT and OT risks across the entire maritime supply chain.

Strategic Directions for Policy and Research

To effectively close these gaps and strategically boost resilience, future policy and research efforts must zero in on specific, actionable areas.

Table 1: Strategic policy and research directions for maritime cybersecurity

Focus Domain	Proposed Intervention	Proposed Framework
Regulation	Harmonisation and Mandatory Standards	Develop an internationally binding cybersecurity code (akin to the ISPS Code for physical security) to establish a common, auditable baseline across all flag and port states.
Data & Reporting	Incentivised or Mandatory Reporting	Establish a secure, anonymised global clearinghouse for cyber incident data, protected by anti-trust waivers, to facilitate faster, more accurate threat intelligence sharing across the sector.
Insurance	Developing Specific Cyber Insurance Products	Research and develop standardised, affordable cyber insurance models that clearly delineate coverage (e.g., between acts of war and cyberterrorism) to promote better risk transfer and incentivise security investment.
Technology	OT-Specific Resilience Research	Focus heavily on the survivability and recovery of core Operational Technology systems (e.g., ECDIS, engine control) and the development of future autonomous, inherently cyber-resilient vessel systems.

Recommendations and Conclusion

Conclusion

A thorough review of recent literature strongly confirms that the maritime industry is at a critical turning point. While technological advancements—driven largely by the rapid digital transformation to Shipping 4.0—have brought considerable benefits, they have simultaneously and dramatically increased the industry's exposure to sophisticated cyber threats (Li *et al*., 2024; Progoulakis *et al*., 2021; Zarzuelo, 2020). This evolution has resulted in the merging of Information Technology and Operational Technology systems into interconnected Cyber-physical Systems, which are now essential for the safe and efficient operation of modern vessels and vital port infrastructure (Li *et al*., 2024; Progoulakis *et al*., 2021).

Our analysis has specifically identified core operational systems, including AIS, GNSS, ECDIS, VDR, RADAR, VSAT, and GMDSS, as having significant, exploitable vulnerabilities. For instance, the Electronic Chart Display and Information System presents particular, complex cyber risks related to its underlying operating system and backup arrangements (Ashraf *et al*., 2022; Li *et al*., 2024; Sviličić *et al*., 2019). Similarly, the reliance on satellite navigation systems like GPS/GNSS has exposed vessels to fundamental threats such as precise signal spoofing (Androjna *et al*., 2020; Farah *et al*., 2022; Silverajan *et al*., 2018).

A consistent finding from analysing cyber incidents is that attacks in the maritime sector are typically low in frequency but have devastatingly high impacts. This combination makes them exceptionally difficult to predict, defend against, and prepare for financially. The diverse techniques and motivations among various threat actors further suggest that no single, simplistic solution exists to comprehensively tackle the problem (Dominguez-Péry *et al*., 2023; Li *et al*., 2024; Meland *et al*., 2021; Sesay, 2019). While the regulatory framework, primarily the IMO Guidelines on Maritime Cyber Risk Management, has mandated integrating cyber risk into safety management systems, this is an ongoing, evolving process that requires a fundamental shift in organisational mindset and greater accountability from manufacturers to improve the inherent security of their products. A significant and persistent vulnerability gap remains in cybersecurity awareness, particularly within the economically crucial port sector (Bocayuva, 2021).

Recommendations and Future Research Directions

Based on this critical review of the threats, economic impacts, and policy gaps, the following strategic recommendations are proposed to decisively enhance the maritime sector's cybersecurity posture, alongside key directions for essential future research.

Strategic and Organisational Recommendations

Adopt a Holistic Risk Management Approach

Maritime cybersecurity must urgently move beyond a fragmented, IT-centric approach to implement a holistic, ecosystem-wide strategy. This strategy should systematically address the entire supply chain, from shipboard systems to shore-based infrastructure. Stakeholders need to develop and rigorously implement effective preventive and corrective strategies to mitigate potential systemic impacts.

Standardised Framework Implementation

The mandatory adoption of robust, proven security frameworks, such as the NIST Cybersecurity Framework v2.0, is strongly recommended. This provides a standardised, repeatable guide for comprehensive analysis and the implementation of appropriate cybersecurity baseline controls across the entire industry.

Focus on Critical Infrastructure Protection

Policymakers must collaborate intensely with the private sector to ensure that critical port infrastructure is adequately protected

against the highest-impact cyber threats, while simultaneously ensuring that regulatory burdens do not hinder the secure development of new technologies.

Technical and Methodological Recommendations

Mandatory Use of Tailored Risk Assessment Methodologies

Implement sophisticated, maritime-specific risk assessment methods. Techniques like STRIDE and DREAD for qualitative/quantitative analysis, or hybrid models (such as combining FMEA with Rule-based Bayesian Networks), should be mandated to understand better and probabilistically evaluate complex IT/OT threat levels.

Utilise Proactive Testing and Assessment Tools

System engineers should be required to use specialised, validated tools like the BRidge Attack Tool for systematic security assessments of integrated bridge systems, especially during the design and development phases, to identify vulnerabilities early.

Develop Cybersecurity Testbeds

Targeted public and private investment in virtual testbeds, such as the open-source MaCySTe, which accurately reproduces the onboard cyber-physical system network, must be strongly encouraged. These testbeds are crucial for realistic security testing, countermeasure development, and high-fidelity staff training.

Future Research Directions

Resilience and Survivability of Autonomous Vessels

Future research must urgently focus on the survivability and secure operation of autonomous vessels when faced with sophisticated cyber-attacks. This includes developing and testing advanced security architectures, such as the Zero-Trust security framework for device authentication and network access.

Infrastructure Resilience for Maritime Autonomy

Further exploration is vital into how concepts of resilience and lessons learned from other established transport modes (e.g., the importance of intelligent infrastructure support in aviation) can be effectively adapted to enhance the resilience of maritime autonomy systems.

Closing Policy and Economic Gaps

Research must continue to identify and propose policy updates and new enactments that specifically address the pervasive economic and supply chain aspects of maritime cybersecurity. This includes the ongoing quantification of the true economic burden of cyber risk on trade and insurance costs, directly addressing the core research gap identified in this paper.

Acknowledgements

I would like to express my gratitude to UniKL MIMET for providing the academic environment and library resources necessary to conduct this review. Access to these specialised maritime databases was instrumental in completing this paper. I am also grateful to my colleagues and peers within the Master of Maritime Operations and Management program for their encouragement and for the insightful discussions that helped shape the perspectives in this work. Finally, I wish to thank my family for their constant support and understanding during my pursuit of this postgraduate degree.

Conflict of Interest Statement

The author declares that they have no conflict of interest.

Author Contributions Statement

The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

References

Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean and Coastal Management*, *236*, Article 106493. https://doi.org/10.1016/j.ocecoaman.2023.106493

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network*, *2*(1), 123–138. https://doi.org/10.3390/network2010009

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, *8*(10), Article 776. https://doi.org/10.3390/jmse8100776

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A survey on cyber security threats in IoT-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2677–2690. https://doi.org/10.1109/TITS.2022.3164678

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, *13*(1), Article 22. https://doi.org/10.3390/info13010022

Bocayuva, M. (2021). Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic. *WMU Journal of Maritime Affairs*, *20*, 173–192. https://doi.org/10.1007/s13437-021-00240-4

Bolbot, V., Kulkarni, K., Brunou, P., Valdez Banda, O., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, *39*, Article 100571. https://doi.org/10.1016/j.ijcip.2022.100571

Clavijo Mesa, M. V., Patino-Rodriguez, C. E., & Guevara Carazas, F. J. (2024). Cybersecurity at sea: A literature review of cyber-attack impacts and defenses in maritime supply chains. *Information*, *15*(11), Article 710. https://doi.org/10.3390/info15110710

de la Peña Zarzuelo, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transport Policy*, *100*, 1–4. https://doi.org/10.1016/j.tranpol.2020.10.001

Dimakopoulou, A., & Rantos, K. (2024). Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2.0. *Journal of Marine Science and Engineering*, *12*(6), Article 919. https://doi.org/10.3390/jmse12060919

Dominguez-Péry, C., Arab, K., Perea, C., & Tassabehji, R. (2023). Ship's cyber security: Antecedents to improve resilience capabilities and their impact on decision-making and collaborative performance. *MCIS 2023 Proceedings*, Article 34. https://aisel.aisnet.org/mcis2023/34

Hemminghaus, C., Bauer, J., & Padilla, E. (2021). BRAT: A BRidge Attack Tool for cyber security assessments of maritime systems. *TransNav: The International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(1), 35–44. https://doi.org/10.12716/1001.15.01.02

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), Article 1860. https://doi.org/10.3390/s22051860

Johnsen, S. O., & Kilskar, S. S. (2020). A review of resilience in autonomous transport to improve safety and security. In Baraldi, P., Di Maio, F., & Zio, E. (Eds.), *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*. Research Publishing. https://www.sintef.no/globalassets/project/hfc/sarepta/johnsen-kilskar-2020-a-review-of-resilience-in-autonomous-transport-to-improve-safety-and-security.pdf

Kavallieratos, G., & Katsikas, S. (2020). Managing cyber security risks of the cyber-enabled ship. *Journal of Marine*

Science and Engineering, *8*(10), Article 768. https://doi.org/10.3390/jmse8100768

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, *37*, Article 100526. https://doi.org/10.1016/j.ijcip.2022.100526

Li, M., Zhou, J., Chattopadhyay, S., & Goh, M. (2024). *Maritime cybersecurity: A comprehensive review* [Preprint]. arXiv. https://arxiv.org/abs/2409.11417v3

Longo, G., Orlich, A., Musante, S., Merlo, A., & Russo, E. (2023). *MaCySTe: A virtual testbed for maritime cybersecurity* (SSRN Scholarly Paper No. 4374685). Social Science Research Network. https://doi.org/10.2139/ssrn.4374685

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav: The International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(3), 519–530. https://doi.org/10.12716/1001.15.03.04

Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis: How to reduce threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Park, C., Kontovas, C., Yang, Z., & Chang, C.-H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean and Coastal Management*, *235*, Article 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering*, *9*(12), Article 1384. https://doi.org/10.3390/jmse9121384

Sesay, M. A. K. (2019). *Awareness of cybersecurity threats in the Port of Freetown, Sierra Leone* [Master's dissertation, World Maritime University]. WMU The Maritime Commons. https://commons.wmu.se/cgi/viewcontent.cgi?article=2457&context=all_dissertations

Silverajan, B., Ocak, M., & Nagel, B. (2018). Cybersecurity attacks and defences for unmanned smart ships. In *2018 IEEE Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 15–20). IEEE. https://doi.org/10.1109/Cybermatics_2018.2018.00037

Svilicic, B., Brčić, D., Žuškin, S., & Kalebić, D. (2019). Raising awareness on cyber security of ECDIS. *TransNav: The International Journal on Marine Navigation and Safety of Sea Transportation*, *13*(1), 231–236. https://doi.org/10.12716/1001.13.01.24

Symes, S., Blanco-Davis, E., Graham, T., Wang, J., & Shaw, E. (2025). The survivability of autonomous vessels from cyber-attacks. *Journal of Marine Engineering & Technology*, *24*(3), 194–216. https://doi.org/10.1080/20464177.2024.2428022

Tam, K., Moara-Nkwe, K., & Jones, K. D. (2021). The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. *Maritime Technology and Research*, *3*(1), 16–30. https://doi.org/10.33175/mtr.2021.241410

Yoo, Y., & Park, H.-S. (2021). Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. *Journal of Marine Science and Engineering*, *9*(6), Article 565. https://doi.org/10.3390/jmse9060565