30th
International Maritime Lecturers Association Conference
Split Croatia
www.imla30.org

International Maritime Lecturers Association
FACULTY OF MARITIME STUDIES

STRENGTHENING CYBER RESILIENCE AT SEA: CROSS-SECTORAL INSIGHTS FOR MARITIME RISK MITIGATION

Lakhvir Singh[1*], Reza Ziarati[1], Vanessa Makker[1], German de Melo Rodriguez[2], Janne Lahtinen[3], Izabela Bodus-Olkowska[4], Konstantinos Karampidis[5], Manos Vasilakis[5], Aris Chronopoulos[6], Andrei Bautu[7], Monika Klein[8], Tomaz Gregoric[9]

[1] Centre for Factories of the Future, Business Intelligence Division, Alingsas, Sweden
[2] Faculty of Nautical Studies of Barcelona, Barcelona, Spain
[3] Satakunta University of Applied Sciences, Rauma, Finland
[4] Maritime University of Szczecin, Institute of Maritime Technology, Szczecin, Poland
[5] Hellenic Mediterranean University, Heraklion, Greece
[6] IDEC S.A., 96, Iroon Polytechniou Avenue, 18536 Piraeus, Greece
[7] Romanian Naval Academy, Constanta, Romania
[8] Berlin School of Business and Innovation, Berlin, Germany
[9] Spinaker, Portorož, Slovenia
* **Corresponding author:** lakhvir.singh@c4ff.se

https://doi.org/10.7225/imla30.51

Abstract. The accelerated digitalization of the maritime sector has increased exposure to cyber threats, calling for the creation of sector-specific cyber resilience strategies. This study feeds into the CyberSEA project, an EU-funded research project involving the cooperation of partners from eight European countries, each conducting national-level research to assess vulnerabilities of maritime cybersecurity and the necessary training requirements. The main goal of this investigation is to identify cybersecurity gaps existing in maritime systems and to distill lessons from other critical sectors, to inform the creation of tailored risk mitigation strategies transferable to the maritime domain. The methodology used follows a multi-stage approach. Desk research was conducted by each national partner to outline the current cyber threats in maritime environments along with the existing defense practices. This was followed by a comparative analysis of cybersecurity practices taken up in sectors such as finance, education, healthcare, and logistics. Furthermore, a focus group of cybersecurity practitioners from partner countries was consulted to validate the findings and place risks relevant to the maritime sector. Finally, a modular training program was designed to fill the gaps identified. The findings indicated ongoing weaknesses in shipboard networks, port facilities, and human factors. The findings reflected, in particular, that while technical safeguards are available, a significant lack of cyber awareness and scenario-based training of maritime personnel persists. Lessons from other sectors highlighted the value of proactive threat modeling, regulatory harmonization, and continuous training activities. The study ultimately argues that enhancing maritime cybersecurity requires a holistic and multidisciplinary solution combining technical, organizational, and educational measures. The CyberSEA project illustrates the value of international collaboration in developing scalable and adaptable training programs with both local relevance and applicability to common industry issues.

Keywords: Maritime Cybersecurity; Cyber Risk Management; Cross-Sector Analysis; CyberSEA Project; Digital Resilience; Maritime Training.

1. INTRODUCTION

The accelerated digitalization of the maritime industry has exposed it to cyber threats, underscoring an urgent need for sector-specific cyber resilience strategies. This study is a part of the CyberSEA project, an EU-funded initiative involving nine partners from eight European countries, each working at the national level to study maritime cybersecurity vulnerabilities and training needs. The primary goal of this investigation is to identify cybersecurity weaknesses in maritime systems and bring in lessons learned from other critical sectors for tailored strategies to mitigate risks in the maritime domain. Our methodology employs a multi-phase process:

- Each national partner performed a desk study to map the most common maritime cyber threats and defense frameworks in place.
- This was followed by a comparative analysis of cybersecurity strategies applied in other sectors like finance, education, healthcare, and logistics.
- A focus group comprising cybersecurity professionals from partners' countries were convened to validate findings and help contextualize risks from a maritime perspective.

The factors present recurrent vulnerabilities in shipboard networks and port infrastructure and a human factor in all cases. The key results indicate that while certain technical safeguards are in place, there is a strong deficiency in cyber awareness and scenario-based training for maritime personnel. Furthermore, lessons derived from other sectors strongly emphasize the importance of proactive threat mitigation. To address these challenges, this study aims to strengthen cyber resilience in the maritime sector by learning from other critical industries and developing focused training programs. With this in mind, the research is guided by three main questions:

1. What cybersecurity approaches used in sectors like finance, healthcare, and logistics might be adapted for use in maritime operations?
2. Given the unique operational, technical, and regulatory realities of the maritime domain, how can these cross-sector practices be practically applied?

2. GLOBAL MARITIME TRANSPORT SYSTEM

The Global Maritime Transport System (GMTS) is a backbone for international trade which facilitates the movement of goods across continents. Maritime transport thus historically stands for 80% of all cargo volumes globally, emphasizing the case for maritime shipping in the global economy (Drewry, 2020). In terms of trade value, the maritime sector accounts for about 70% of global commerce, showcasing its importance not just in terms of volume but also in economic impact (Smith & Taylor, 2021). Given the heavy dependence on maritime infrastructure, it's clear that the sector needs strong cybersecurity measures in place, especially as shipping operations become more digital and interconnected.

The maritime transport system is a complex, interrelated system made up of different parts such as vessels, ports, shipping firms, inland waterways, intermodal transfer points, and the labor force in charge of managing and maintaining operations. As depicted in Figure 1, this environment operates as an integrated system, whereby every subsystem plays an important role in ensuring smooth transportation of commodities and people across the maritime and land areas (Kessler & Shepard, 2022). Vessels form a critical part of this system, serving a range of important functions, ranging from onboard networking, navigation and communication systems, manufacturing processes, maintenance activities, and disposal operations. Growing dependence on sophisticated technologies improves their operational efficacy and safety; however, this dependence also makes them vulnerable to cyber-attacks (Tam & Jones, 2018; Katsikas et al., 2021). Despite the increasing awareness of cyber threats, the maritime sector continues to experience numerous cyber incidents targeting both IT and OT infrastructure. Vaarandi et al. (2025) confirm this trend, stating, "In recent years, many cyber incidents have occurred in the maritime sector, targeting the information technology (IT) and operational technology (OT) infrastructure." This necessitates a focused approach to security, including robust monitoring mechanisms.

Shipping operators are responsible for managing the commercial and logistical aspects of maritime transport, which include baggage and cargo handling, financial transactions, communication management, reservations, and scheduling operations. These operations are supported by interconnected digital infrastructure systems that remain vulnerable to cybersecurity threats if not properly secured (Jones, Tam, & Papadaki, 2016). The human aspect of the maritime transport structure includes a heterogeneous group of stakeholders, including crew members, suppliers, trading partners, and customers. Every one of the stakeholders involved in the intricacies of maritime trade carries great responsibilities; however, they also bring in probable cybersecurity threats through means like social engineering, supply chain weaknesses, and inadequate security consciousness

Figure 1. Overview of the Maritime Transportation System and Its Interdependencies. (Kessler and Shepard, 2022)

(Katsikas et al., 2021). Ports are integral nodes in the structure, facilitating logistics, marine infrastructure, and real-time commercial activities. In addition, they manage communication and traffic management systems that are critical in the successful coordination of ship arrivals and departures, as well as cargo transfers (DNV GL, 2016). Due to their pivotal position in world trade and the huge amount of cargo handled, ports are greatly attractive targets for cybercriminal activity (International Maritime Organization, 2021).

The GMTS further includes inland waterways, which involve dredging, maintenance activities, and the management of Aids to Navigation (ATONs) to provide safe navigation and access to port facilities. Further, intermodal transfers couple maritime transportation with other transportation modes, including barges, airlines, railway systems, and trucking companies. These linkages highlight the system's dependence on global logistics infrastructures, demonstrating the cascading effects that cyber-related disruptions to one area can have on the overall transportation network (Kessler & Craigen, 2016). The representation highlights the significance of maritime cybersecurity, which goes beyond individual ships to include port terminals, inland transport links, intermodal logistics networks, and the vast range of individuals and organizations involved in these processes. The complex nature and interdependencies of these elements call for an integrated cybersecurity strategy to strengthen the resilience of the overall supply chain, as opposed to focusing only on standalone assets. According to Katsikas et al. (2021), the strategy must include technical solutions, governance structures, educational programs, and cross-industry collaborations to efficiently counter the ever-changing cyber threats.

Most container ships are typically designed to last around 20 to 30 years. But with the right care and occasional upgrades, many of these vessels can keep sailing long after that. The aging of the global fleet has become a major issue for the GMTS, especially when it comes to cybersecurity. As ships get older, they often hang on to outdated systems that don't align with today's cybersecurity standards, making them more susceptible to cyber threats. According to Johnson and Lee (2019), 38% of oil tankers and 59% of general cargo ships currently in operation are over 20 years old, which really underscores the aging infrastructure problem in the industry. This increasing number of older vessels raises the risk level, as outdated technology and limited digital defenses

can leave critical maritime operations open to potential cyberattacks.

Modern shipping vessels are complex cyber-physical systems that consolidate a wide variety of digital, operational, and communicative subsystems to facilitate the efficient and safe transport of goods along international maritime trade routes. As Figure 2 illustrates, these vessels are based on a coherent structure of interdependent subsystems that augment navigation, communication, crew management, cargo monitoring, and ship stability in a combined manner. The central concern of the vessel network is in the administration and operation of core functions, which include customs and immigration procedures, internal time management, and electronic correspondence. On the other hand, the crew network offers basic services with the aim of promoting crew welfare, including access to entertainment, electronic mail, and wired and wireless internet connectivity; such services are important in maintaining morale and productivity over long journeys (Tam & Jones, 2018).

The Integrated Navigation System (INS) is a cornerstone of modern maritime operations, directly supporting the Officer of Watch (OOW) in safe navigation. However, the multifaceted nature of the INS also exposes it to significant cyber risks. As highlighted by Oruc et al. (2025), "The INS comprises several components that may be susceptible to cyber-attacks, hence it faces cyber risks that need to be mitigated." Understanding these vulnerabilities is paramount for developing effective countermeasures. The navigation apparatus fitted on ships is responsible for ensuring maritime safety through the use of Electronic Chart Display and Information Systems (ECDIS), Global Navigation Satellite Systems (GNSS), radar technology, and meteorological observation equipment to aid real-time decision-making and route planning (Kessler & Craigen, 2016). In addition, communication networks are vital to safety and operational coordination, using Automatic Identification Systems (AIS), GSM networks, radio communication, satellite communication, and ship-to-ship and shore-based communications, including Voice over IP (VoIP) technologies to ensure seamless connectivity (DNV GL, 2016).

The ship's network backbone supports its cyber infrastructure using diverse technologies, such as closed-circuit television (CCTV), firewalls, internet services, intercom systems, synchronized master clocks, public address systems, remote management interfaces, and a segmented device management approach that helps isolate sensitive parts while strengthening cybersecurity (Tam & Jones, 2018).

Industrial control systems (ICS) play a crucial role in the operational structure of the ship, controlling numerous functions such as cargo handling, propulsion, steering, sensor integration, and the human-machine

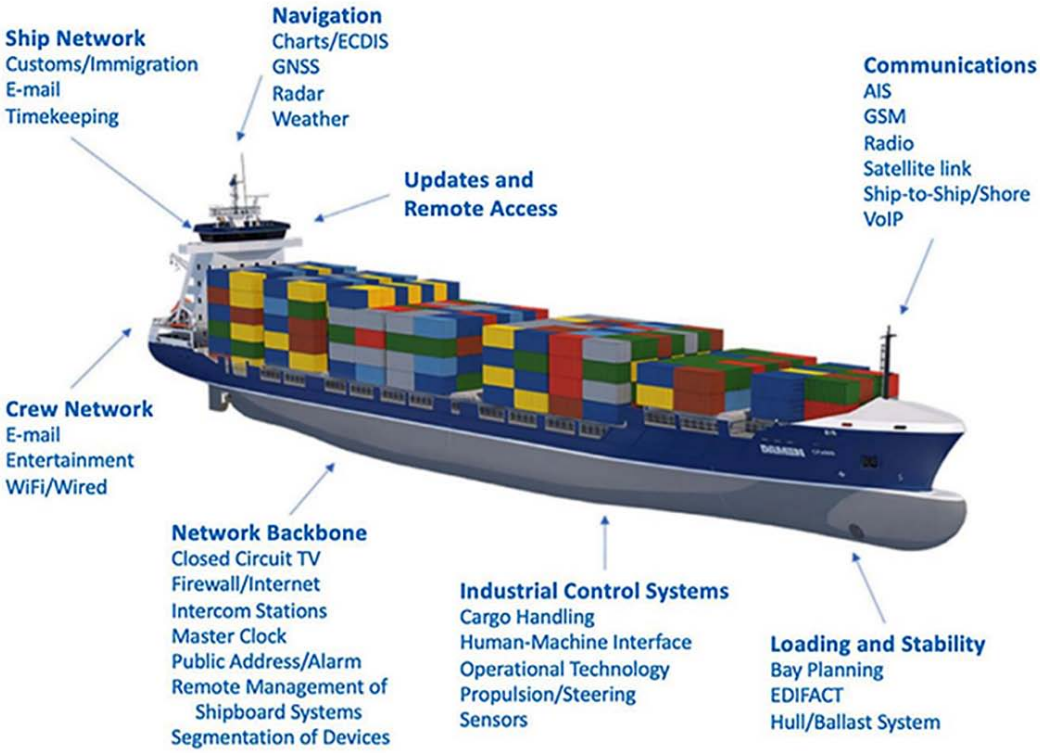

Figure 2. Cyber-Physical System Components of a Modern Vessel. (Source: Atlantic Council)

interface, which involves real-time monitoring of physical processes (Jones, Tam, & Papadaki, 2016). The networked environment and reliance on real-time information have increased the exposure of the systems to cyber-attacks (Katsikas et al., 2021).

Additionally, loading and stability mechanisms are instrumental to effective cargo distribution and the maintenance of balance in ships. This is enabled by technologies like bay planning software, Electronic Data Interchange for Administration, Commerce, and Transport (EDIFACT), and automated hull and ballast management systems (International Maritime Organization, 2021). Greater dependence on software updates and remote accessibility for maintenance, system configuration, and cybersecurity updates increases ship vulnerability to cyber-attacks since poor access controls or slowness in updating may leave systems vulnerable to exploitation (Katsikas et al., 2021; Tam & Jones, 2018). The interconnectedness of these maritime subsystems poses significant challenges in terms of cybersecurity. A weakness in one system can spread to the entire network of the ship, thus impacting vital shipboard operations such as navigation, propulsion, and cargo handling (Kessler & Craigen, 2016). It is, therefore, necessary to establish robust cybersecurity measures that include network segmentation, access control, continuous monitoring, and incident response plans specific to the maritime environment, to protect shipboard cyber-physical systems. It is often recommended to utilize a multi-layered defense approach that incorporates technical, procedural, and organizational security elements to successfully address the unique threat profile faced by modern ships (Katsikas et al., 2021).

3. LITERATURE REVIEW

As maritime operations increasingly depend on digital technologies, like onboard networks, integrated navigation systems, and port logistics platforms, the potential for cyber threats has grown significantly (IMO, 2021; ENISA, 2022). As Oruc et al. (2025) note, "As maritime operations become increasingly reliant on interconnected information technology (IT) and operational technology (OT) systems, ensuring cybersecurity on vessels has become more critical than ever". Recent research has pointed out various cyber vulnerabilities within maritime systems, such as outdated software, weak encryption methods, insufficient network segmentation, and poor access control (Tam & Jones, 2019; CyberKeel, 2020). These technical issues are often made worse by a lack of investment in cybersecurity training and awareness among maritime staff (Cariou et al., 2020). This is especially worrying given the aging fleets, where ships can stay in service for over 20 to 30 years. Johnson and Lee (2019) estimate that 38% of oil tankers and 59% of general cargo ships are over 20 years old, which raises the chances of outdated and insecure systems still being in use. The combination of these factors creates a maritime environment that is not only susceptible to opportunistic attacks but also to targeted cyber operations from state-sponsored or criminal actors.

Back in 80s, hacking was all about having serious technical know-how. The tools were pretty basic and pulling off a cyberattack required a solid grasp of programming, networking, and systems. Hackers had to roll up their sleeves and create custom scripts or manually find and exploit vulnerabilities, which made the whole process both time-consuming and demanding in terms of skill. Fast forward to today, and things have changed dramatically. With the rise of advanced hacking tools, even those with just a little technical knowledge can launch significant cyberattacks using ready-made solutions. Nowadays, you've got "plug-and-play" hacking kits, ransomware-as-a-service, and automated scripts that make it easier than ever to break into systems. This shift has really opened the floodgates for cyber threats, leading to a surge in cybercrime activity. Figure 3 highlights the common cybersecurity vulnerabilities in the maritime industry.

Efforts to tackle these risks have resulted in the release of various guidelines and frameworks. The International Maritime Organization (IMO) put forth its guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3), suggesting that cybersecurity should be woven into existing safety management systems (IMO, 2021). On a regional scale, the EU has pushed forward legislation like the NIS Directive and its successor, NIS2, aimed at enhancing cybersecurity readiness across critical sectors, including maritime transport (European Commission, 2022). Industry groups such as BIMCO and INTERTANKO have also created best practice documents to help shipping companies adopt essential cyber hygiene measures. However, there's evidence that compliance is still hit or miss, especially among smaller maritime operators (ENISA, 2022).

To boost resilience, experts and scholars are advocating for a more comprehensive, cross-sector approach. Studies comparing different sectors have revealed that industries like aviation and finance are ahead in rolling out advanced cybersecurity strategies. For instance, aviation regulators require incident reporting and scenario-based simulation training for airline operators (ICAO, 2021), while the financial sector has taken the lead in real-time threat intelligence sharing and strict regulatory compliance through standards like ISO/IEC 27001 (ISO, 2013). The energy

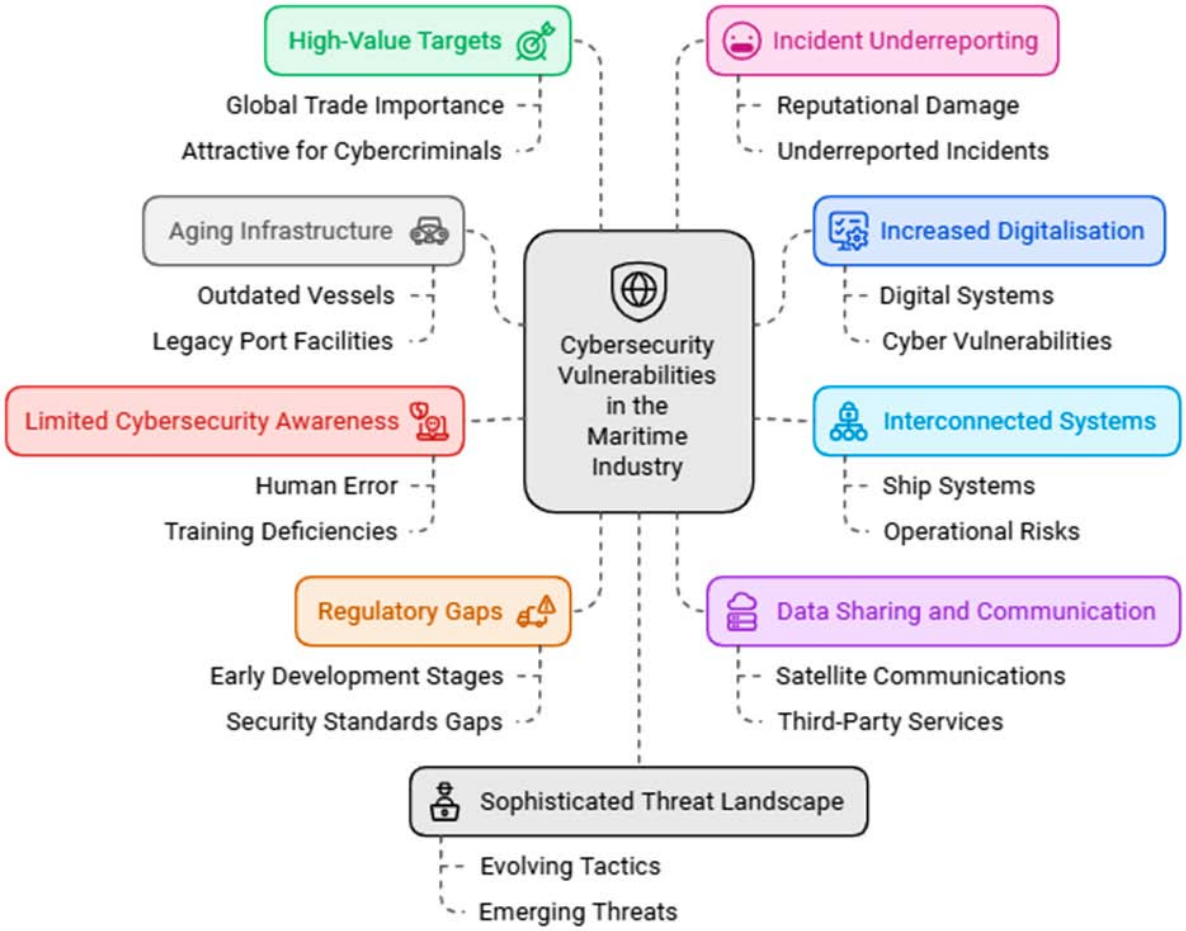

Figure 3. Why is the Maritime Industry so Vulnerable to Cyberattacks?

sector has also adopted advanced risk assessment tools and coordinated frameworks across the industry (ENISA, 2021). Learning from these sectors could provide valuable insights for the maritime industry, which still lacks cohesive, industry-wide threat modeling systems and unified response protocols.

The literature highlights a significant gap in standardized cybersecurity training specifically designed for maritime personnel. Most training programs are quite haphazard, relying little on interactive, scenario-based learning tools (BIMCO, 2021; Greidanus & van den Berg, 2018). Additionally, the human factor remains the weakest link in maritime cybersecurity, with phishing, credential theft, and social engineering being some of the most prevalent attack methods (Tam & Jones, 2019). As a result, there's an increasing acknowledgment of the necessity for modular, scalable training curricula that effectively cover technical skills, organizational readiness, and behavioral awareness in a cohesive way.

Current approaches to threat modeling and risk assessment in ship cybersecurity exhibit notable inconsistencies, as revealed by recent systematic reviews. Erbas et al. (2024) conducted such a review and concluded that "Significant inconsistencies were observed in current approaches, underscoring the urgent need for standardized threat modeling and risk assessment frameworks that consider the special requirements of autonomous ships." This emphasizes a critical need for unified methodologies to accurately assess and mitigate cyber risks in this evolving domain.

In short, while digitalization has led to operational improvements in maritime logistics and navigation, it has also brought about serious cybersecurity challenges. Current efforts to tackle these threats are still quite fragmented and underdeveloped, especially when compared to other high-reliability sectors. The literature emphasizes the need for a cross-sectoral, multidimensional approach to maritime cybersecurity, one that not only focuses on technical defenses but also on organizational governance and workforce preparedness. These insights have played a crucial role in shaping the CyberSEA project and its multi-phase research methodology.

4. METHODOLOGY

This study took a structured, multi-phase approach to dive into the vulnerabilities of maritime cybersecurity. It aimed to gather insights from other critical infrastructure sectors and create a focused training framework specifically for the maritime field. The project was a collaborative effort involving national partners from eight European countries, all part of the EU-funded CyberSEA initiative, which helped ensure that the methodology was both relevant and rigorous. The research unfolded in five interconnected phases.

The first phase was all about desk research, where each national partner investigated maritime cybersecurity threats and the existing defense mechanisms in their own countries. This involved reviewing maritime cyber incident databases (like EMSA, 2021), industry guidelines from organizations such as BIMCO and the International Maritime Organization (IMO, 2021), national regulations, and academic studies. To keep things consistent and comparable, a standardized data collection template was used by all partners.

In the second phase, a comparative analysis was conducted on cybersecurity strategies across sectors (including telecom, construction, education, logistics, and technology). These sectors were chosen for their digital maturity, history of cyber incidents, and robust regulatory frameworks. The focus here was on pinpointing best practices in threat modeling (ENISA, 2022), regulatory compliance (European Commission, 2016), incident response, and workforce development initiatives.

The third phase brought together findings from both the national maritime assessments and the cross-sector comparisons to create a comprehensive vulnerability profile for maritime systems. The analysis revealed ongoing challenges with outdated shipboard systems, cybersecurity in port infrastructure, and risks related to human factors, echoing concerns raised in earlier studies (Cariou et al., 2020; Tam & Jones, 2019). To further validate and contextualize these findings, a focus group was organized as part of the fourth phase. Fifth and final phase involved detailed documentation of the findings and results.

5. CROSS-SECTOR BEST PRACTICES EXTRACTED

While cross-sectoral comparisons reveal valuable cybersecurity practices from digitally mature industries, these insights must be critically evaluated and thoughtfully adapted to the unique operational context of maritime environments. To avoid generic or inappropriate transfer, this study employs an Extraction–Translation–Integration (ETI) framework.

First, cybersecurity practices proven effective in sectors such as finance, healthcare, and logistics are **extracted**. Second, these practices are **translated** through careful consideration of maritime-specific constraints, including vessel mobility, intermittent connectivity, and heterogeneous crew expertise. Finally, the adapted practices are **integrated** by aligning them with maritime procedures, training protocols, and technological infrastructure. For instance, real-time threat detection systems from the finance sector may be adapted into intermittent but intelligent anomaly monitoring onboard ships, complemented by hybrid training modules tailored to maritime stakeholders. This structured approach facilitates the practical operationalization of cross-sector insights, ensuring they are conceptually relevant, technically feasible, and organizationally compatible within the maritime domain.

6. FINDINGS

The research findings indicate that the maritime sector's digital transformation has created complex cybersecurity challenges that require strategic, multi-layered responses. By analyzing cybersecurity frameworks and best practices from highly regulated and digitized sectors such as finance, education, fintech and healthcare, from partners countries, this study identified transferable strategies that can be contextualized and applied to maritime operations. The analysis resulted in the proposal of a comprehensive cybersecurity framework that addresses policy, governance, technical, and human factors within maritime environments.

6.1. Cybersecurity Policies and Governance

A recurring finding from cross-sectoral benchmarking is the centrality of strong governance and formalized policies in cybersecurity risk mitigation. Both the fintech and healthcare sectors operate under stringent compliance regimes, including adherence to ISO/IEC 27001 and NIST cybersecurity frameworks, ensuring systematic risk assessment, incident response planning, and data protection (ISO, 2013; NIST, 2020). In contrast, although the maritime industry has adopted the IMO Guidelines on Maritime Cyber Risk Management (IMO, 2021), implementation has often lacked consistency and contextual specificity.

6.2. Access Control and Authentication

Securing access to maritime digital infrastructure is a critical concern. Finidngs from the finance sector

indicate that Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) significantly reduce risks of unauthorized access (ENISA, 2021).

6.3. Data Protection and Encryption

In high-stakes industries, such as healthcare, data encryption is non-negotiable due to the sensitivity of personal and operational information. Systems like AIS, ECDIS, and satellite communication modules are especially vulnerable to data interception and manipulation.

6.4. Incident Response and Security Monitoring

Effective cybersecurity involves not just prevention but also timely detection and response. Fintech and critical infrastructure sectors leverage Security Information and Event Management (SIEM) systems and conduct regular cyberattack simulation drills to test and refine response strategies. These practices were found to be minimally implemented within maritime organizations.

6.5. Employee Training and Awareness

The human factor remains a persistent vulnerability across all sectors, but targeted training and awareness campaigns have shown measurable benefits in reducing incidents caused by social engineering and user error (Greidanus & van den Berg, 2018).

6.6. Network Security and Segmentation

Network segmentation and perimeter defenses were among the most effective practices observed in non-maritime critical sectors.

6.7. Vulnerability Management

Regular vulnerability scanning and timely patching are essential practices that remain underdeveloped in maritime environments, particularly for OT systems that are often disconnected from real-time update channels.

6.8. Third-Party Vendor Risk Management

Outsourcing software, satellite communication, and technical maintenance to third-party vendors introduces an additional attack vector. Sectors such as fintech and healthcare require strict compliance and conduct regular audits of their vendors.

6.9. Mobile Device Management (MDM) and BYOD Policies

With increasing use of smartphones and tablets onboard for communication, navigation, and diagnostics, the need for Mobile Device Management (MDM) has grown significantly. Other sectors manage this through encrypted storage, VPN-based access, and remote wipe functionality.

These findings underscore the maritime sector's urgent need to adopt a structured, cross-sector-informed cybersecurity framework that is technically robust, operationally feasible, and human-centric. While several maritime-specific standards exist, integration with best practices from other domains provides a broader foundation for building resilience in an increasingly digitized and threat-exposed environment. The table below compares the cybersecurity maturity levels across multiple sectors, Finance, Education, Healthcare, Logistics, and Maritime, based on key control domains identified through desk research conducted by CyberSEA project partners. It highlights where the maritime sector trails and where it can leverage best practices from more advanced industries.

The results of the comparative analysis establish a significant and widespread shortfall in the cybersecurity readiness of the Maritime industry compared with other critical industries like Finance and Healthcare. The analysis shows a significant lag in the deployment of key technical defences, with the Maritime sector recording a 'Low' level of Multi-Factor Authentication (MFA) adoption and a rare ('Rare') use of Security Information and Event Management (SIEM) tools. This is in direct contrast to the 'High' and

Table 1. Comparative Table – Sector vs Maritime Readiness

Control Area	Finance	Education	Healthcare	Logistics	Maritime
MFA Usage	High	Medium	High	Medium	Low
Incident Response Plans	Regularly tested	Varies	Structured and enforced	Mixed	Rarely tested
SIEM Deployment	Yes	Partial	Advanced	Partial	Rare
Staff Training Frequency	Quarterly	Annual	Biannual	Annual	Ad-hoc
Vendor Cyber Assessment	Mandatory	Emerging	Contractual	Formalising	Rarely formal
CISO / Governance Structure	Mature	Developing	Mature	Developing	Fragmented
Cyber Awareness Programmes	Yes	Limited	Yes	Yes	Minimal

'Advanced' levels of adoption in more mature sectors, suggesting that the maritime sector lacks both basic access security practices and the critical monitoring that is essential to identify real-time threats effectively.

This deficiency relates to governance as well as process maturity. The industry's security stance is characterized by a 'Fragmented' governance structure, much as opposed to the 'Mature' CISO-driven operations seen throughout the Finance and Healthcare industries. This structural shortfall is compounded by 'Ad-hoc' staff training, 'Minimal' cyber awareness campaigns, and Incident Response plans that are 'Rarely tested.' Additionally, third-party risk management seems conspicuously lacking, with vendor cybersecurity assessments falling under the banner of 'Rarely formal,' thus highlighting a considerable weakness in the interdependent supply chain of the industry. Taken together, these results point to the Maritime industry's cybersecurity framework as essentially underdeveloped in terms of technology, processes, and human capital, implying a reactive as opposed to proactive approach and making it a singularly vulnerable component of global infrastructure.

As the maritime industry continues to undergo digital transformation, with increasing reliance on shipboard networks, satellite communications, and automated control systems, the risk landscape has evolved beyond traditional physical and environmental threats to include a growing array of cyber risks (Tam & Jones, 2019; ENISA, 2022). One of the most pressing issues identified is the lack of a unified and enforceable cybersecurity governance model within maritime organizations. While the IMO Guidelines on Maritime Cyber Risk Management (IMO, 2021) provide a baseline framework, the practical implementation varies widely across companies and national jurisdictions. This inconsistency undermines resilience at a systemic level. The introduction of dedicated roles, such as Chief Information Security Officers (CISOs), with authority over both IT and OT domains, is not only necessary but already standard practice in other critical sectors. This highlights a clear opportunity for organizational reform and regulatory alignment within maritime enterprises.

The comparative analysis highlighted that while securing access to maritime digital infrastructure remains a critical concern, robust solutions are successfully implemented in other sectors. Specifically, financial sector findings demonstrate that Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) significantly mitigate risks of unauthorized access (ENISA, 2021). To operationalize these proven practices within the maritime domain, it is imperative that maritime systems, including navigation (ECDIS), propulsion, and cargo management software, incorporate these controls. Furthermore, to ensure ongoing security and compliance, regular access audits should be mandated to verify that permissions remain appropriate and reflect any changes in personnel or operational status. This direct application of cross-sectoral best practices would strengthen the maritime industry's cyber posture significantly.

Furthermore, this research demonstrates that while technical solutions such as encryption, network segmentation, and intrusion detection systems are available, their deployment remains uneven. Many vessels, particularly those over 20 years old, operate legacy systems with limited or no cybersecurity capabilities (Johnson & Lee, 2019). This introduces substantial vulnerability across global fleets. Lessons from other sectors show that technical solutions must be complemented by regular vulnerability management and proactive patching cycles, an area where the maritime sector lags due to logistical, operational, and regulatory constraints.

Equally important is the human dimension of cybersecurity. The maritime workforce, often composed of multinational crews with diverse levels of digital literacy, is particularly susceptible to social engineering attacks. The study's findings confirm a marked shortfall in targeted cyber awareness training. Unlike the finance and health sectors—where cyber hygiene is embedded into mandatory compliance routines, maritime organizations often lack structured training programmes. The development of modular, scenario-based curricula, as initiated by the CyberSEA project, is a critical step toward filling this gap and aligning training with operational realities at sea and ashore.

The cross-sectoral approach adopted in this study also underscores the value of interdisciplinary benchmarking. For instance, the fintech sector's rigorous access control policies and healthcare's strict data privacy mechanisms both offer models that can be adapted to shipboard contexts. This comparative method proved highly effective in identifying transferable practices, supporting the argument that maritime cybersecurity must be approached not in isolation, but as part of a broader ecosystem of critical infrastructure protection (NIST, 2020; Greidanus & van den Berg, 2018).

7. DISCUSSION

The research findings collectively highlight the fundamental need for the maritime sector to adopt a systematic cybersecurity approach combining lessons from diverse industries, prioritizing technical applicability, operational feasibility, and human factor

considerations. Even though current regulations specific to the maritime sector form a useful foundation, their blending with best practices in other widely digitized industries renders the overall approach more inclusive and robust.

We have taken from the education, finance, health, and logistics industries a set of cybersecurity best practices that have been successfully applied and yield actionable advice for the maritime sector. They are not only appropriate for shore-side networks but are perfectly transferable as well to address those unique challenges of ships, ports, and shipping enterprises that must operate in remote or bandwidth-limited environments.

- **Governance:** While mature industries have well-established cybersecurity governance, generally a Chief Information Security Officer (CISO) or equivalent to oversee cyber risk management, the maritime sector needs to integrate a dedicated CISO role responsible for both IT and Operational Technology (OT) systems across shipboard and shore facilities. This includes establishing cross-department security committees, clear policies, and internal audit functions to promote accountability and regulatory compliance.
- **Adoption of MFA:** Multi-factor authentication (MFA) is presently a necessary component of secure access control. MFA is mandatory for access to internal networks, cloud services, and remote networks in businesses handling sensitive personal, health, or financial information. MFA is most often paired with passwords, biometrics, one-time tokens, or mobile push authentications. Given the maritime industry's increasing reliance on satellite communication and cloud-based software, the addition of MFA as a complement to passwords, biometric authentication, one-time tokens, or mobile push notifications can significantly enhance security for maritime ships and shore-based facilities.
- **Training Cycles:** Well-structured, periodic training cycles are built into the cybersecurity programs of key industries. Quarterly training, for instance, is conducted and phishing tests are conducted to test awareness and break the complacency of employees. Training modules are normally job function-oriented and accompanied by tests. Maritime organizations, however, still practice ad hoc training, if any, and their personnel are not well-equipped to respond to looming cyber threats.
- **SIEM and IDS Use:** Security Information and Event Management (SIEM) technology and Intrusion Detection Systems (IDS) are in widespread use across key industries for monitoring networks, log management, and real-time anomaly detection. These solutions allow organizations to detect suspicious activity in real time, monitor the origin of breaches, and initiate rapid response. In the technology and financial sectors, SIEM systems are often combined with threat intelligence feeds and automated alerting, giving the ability for proactive security. For the maritime sector, the implementation of SIEM and IDS solutions, even in light or cloud-based form, can assist in providing long-sought visibility into shipboard networks, aid compliance auditing, and enable early warning in the event of cyber-attack.
- **Vendor Evaluations:** Third-party risk is a primary focus area in sectors, like fintech and healthcare, where supply chain vulnerability could threaten information or system integrity. Common practices are pre-contract cybersecurity assessments, including cyber clauses in service contracts, and routine re-evaluations. In the shipping industry, where many contractors and subcontractors work on primary systems, formalized vendor evaluation processes may mitigate a substantial source of risk.

Collectively, these best practices form a multi-layered, proactive cyber security model. Their applicability to the maritime sector is not cut-and-paste, but in the ability to apply them to the sector's operational, regulatory, and cultural landscape. By targeted implementation, the maritime sector can rapidly accelerate its cyber maturity and resiliency.

The figure below depicts CyberSEA framework which proposes concrete measures to enhance maritime cybersecurity based on the lessons directly extracted from the Extraction-Translation-Integration (ETI) framework for maritime security. The CyberSEA project has laid the groundwork for such a framework, combining technical safeguards with organizational policies and continuous training to address identified gaps. The proposed training solution is designed as a modular, role-specific program aimed at enhancing cyber resilience across diverse maritime settings, including shipboard personnel, IT officers, and management teams. Technically, the program includes core modules on threat identification, response protocols, communication during cyber incidents, and system-specific vulnerabilities—such as those related to navigation and propulsion systems. Each module is grounded in realistic maritime scenarios and regularly updated with the latest threat intelligence. Pedagogically, the training employs a blended learning approach that combines e-learning, scenario-based simulations, practical onboard drills, and remote labs. These remote labs provide a virtual, hands-on environment where participants can directly engage with cyber defense tools and practice incident re-

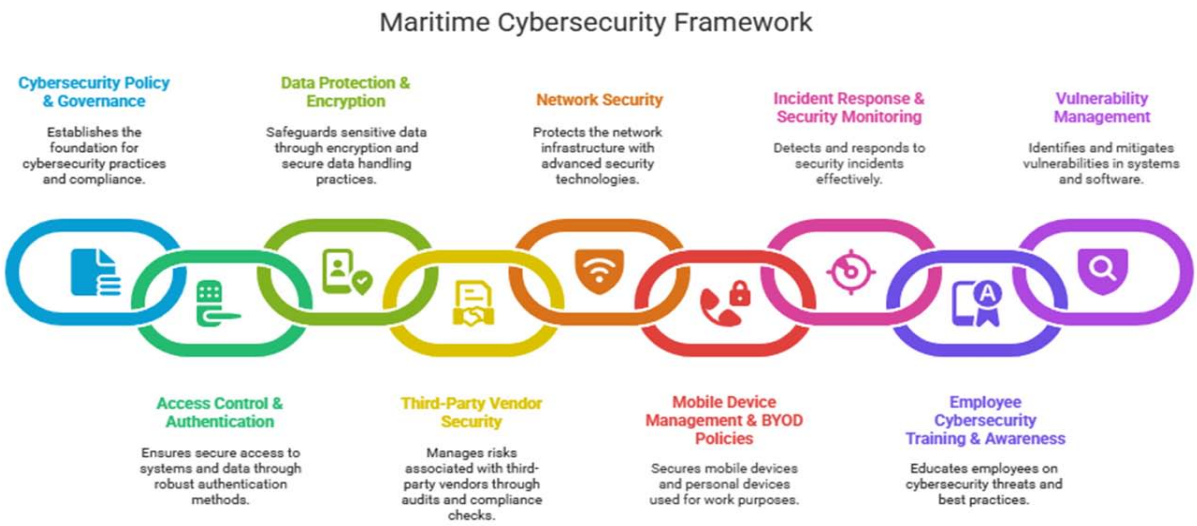

Figure 4. CyberSEA Framework

sponse exercises, enabling practical experience without the limitations of physical location. Assessments include both formative evaluations—such as decision-making exercises embedded in simulations—and summative assessments, including online quizzes and post-exercise debriefings. The modular design allows for scalability and flexibility, with content depth and complexity adjusted based on factors like vessel type, crew experience, and operational environment. Additionally, the program is structured to integrate seamlessly with existing STCW-aligned training frameworks, enhancing its regulatory relevance and facilitating smoother implementation within the maritime industry.

7.1. Cybersecurity Laws and Regulation

Our research findings show that, unlike the strict and formalized compliance models like ISO/IEC 27001 and NIST commonly found in the fintech and healthcare sectors, the shipping industry often lacks homogeneity and context-specific applicability in the implementation of cyber risk management procedures. To bridge this gap, it is crucial to create an industry-specific cybersecurity policy tailored to the shipping sector that meets international requirements as well as accounts for the unique risks associated with shipboard Operational Technology (OT) and navigation systems. Additionally, the governance models should mandate the creation of a Chief Information Security Officer (CISO) or a similar position within shipping operations, with clearly defined duties that cover both IT and OT systems within onboard systems and shore facilities. This centralized model of governance is important to ensure consistent policy enforcement and end-to-end risk management practices.

7.2. Access Control and Authentication

Because of pertinent concerns over access to maritime digital infrastructure, coupled with the widely reported effectiveness of Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) in the financial community, urgent implementation is necessary. For purposes of tightening security, maritime systems like navigation (ECDIS), propulsion, and cargo management applications need to incorporate these strict controls. To meaningfully counter recurring security dangers and respond to changes in personnel or operational conditions, there is a compelling need to mandate periodic access audits that verify permissions are still valid and up to date.

7.3. Data Protection and Cryptography

The overriding significance of data encryption in high-risk industries, including healthcare, coupled with the previously established vulnerabilities of maritime systems, most notably those utilizing AIS, ECDIS, and satellite communication technologies, is in dire need of attention. The maritime sector must embrace rigorous encryption methods, such as AES-256, for data in transit and data at rest, particularly in ship-to-shore facility communications and intra-network transactions (Smith & Taylor, 2021). The immediate implementation of encryption in these vulnerable systems is warranted to safeguard essential operational data.

7.4. Incident Response and Security Surveillance

The fact that efficient incident response and security monitoring procedures are insufficiently executed within maritime entities, especially compared to

proactive methods dominant in critical infrastructure and fintech sectors, highlights a significant lack of resilience. Therefore, there is a need to develop a maritime-specific Incident Response Plan (IRP), which should be complemented by real-time monitoring systems and anomaly detection technologies installed on ships and port facilities. In addition, it is important to ensure that periodic simulation exercises include common maritime threats like ransomware, phishing, and sabotage aimed at systems critical to operational performance (Tam & Jones, 2019), thus enabling the development of response measures within a simulated environment.

7.5. Employee Development and Awareness

Despite the inherent vulnerability inherent in human interaction, focused training and awareness programs have proven successful in reducing incidents across all industries. For the maritime sector to take advantage of this potential, training programs must be tailored to both maritime and shoreside staff, with focus given to realistic scenarios relevant to maritime operations. The use of measures like quarterly phishing tests, mandatory online training modules, and in-person workshops is key to developing a strong cybersecurity culture and raising awareness, thus resulting in an overall improvement in cyber hygiene across the broader workforce.

7.6. Network Segmentation and Security

The success that has been seen in network segmentation and perimeter protection across different non-maritime critical industries can provide valuable lessons for the maritime sector. To enhance resilience, it is essential that firewalls, intrusion detection systems (IDS), and artificial intelligence-enabled traffic analysis are consistently applied across maritime information technology (IT) and operational technology (OT) systems. In addition, it is important to emphasize the importance of separating administrative and operational networks aboard ships and inside port facilities to minimize the threat of intrusions or malware spread and to mitigate the effects of any security breach.

7.7. Vulnerability Management

The underdeveloped state of regular vulnerability scanning and timely patching in maritime environments, particularly for isolated OT systems, poses a substantial risk. Drawing from best practices in healthcare and critical energy systems, maritime organizations must perform regular vulnerability assessments and enforce patch management for SCADA systems, navigation software, and cargo control systems. Crucially, high-risk vulnerabilities should be resolved within 24-48 hours to minimize exploitation windows.

7.8. Third-Party Vendor Risk Management

Dependence on third-party vendors brings significant risks; nonetheless, within the financial technology and healthcare industries, this risk is properly addressed by strict adherence to regulatory frameworks and regular audits. A similar framework should be adopted in maritime operations, requiring third-party vendors to adhere to International Maritime Organization (IMO) guidelines when developing maritime cybersecurity policies. In addition, inclusion of annual security assessments in vendor contracts is critical to promote accountability and reduce supply-chain vulnerabilities (ENISA, 2022).

7.9. Mobile Device Management (MDM) and BYOD Policies

The increasing use of smartphones and tablets aboard ships requires the adoption of robust mobile device management (MDM). The strategy has been used effectively in other industries by leveraging encrypted storage, VPN connectivity, and remote data wiping. The shipping sector needs to embrace strict MDM policies. It is also critical to have enforceable policies for the use of personal devices (BYOD) that limit access to critical systems and ensure exhaustive data encryption.

The collaborative, multinational nature of the CyberSEA project provided unique insights into national-level differences and commonalities in maritime cybersecurity posture. This validates the project's hypothesis that cybersecurity is both a local and global issue. The maritime sector cannot achieve resilience through isolated action. Instead, it requires coordinated efforts among ship operators, port authorities, regulators, technology vendors, and training institutions.

8. CONCLUSION AND RECOMMENDATIONS

This research has bridged a pressing gap in maritime cybersecurity by rigorously exploring shipboard and port system vulnerability and distilling best practice from more technologically advanced sectors. With its phased approach, combining national desk research, cross-sectoral comparison, stakeholder validation, and curriculum development, the CyberSEA project has provided an evidence-based platform for establishing cyber resilience across the maritime sector. The results highlight that while regulatory tools such as the IMO Guidelines provide necessary baseline

direction, operationalization of cybersecurity remains heterogeneous across maritime organizations. Lapses in cyber governance, threat detection, personnel training, and third-party risk management were some of the key areas of weakness. Legacy systems and aging fleets also present additional complexities that are not adequately addressed in prevailing regulatory or organizational strategies.

Basing its approach on cybersecurity best practice in the finance, education, healthcare, and logistics sectors, the research demonstrates the advantage of a cross-industry solution. Sound cybersecurity in these sectors is built on robust governance, tight access control, monitoring in real time, and a company culture of alertness and preparedness. Bringing these principles into maritime environments, taking into account the unique operational and logistical challenges at sea, a viable and scalable solution has been defined. One of the most tangible outputs of this research is the modular training package for building cyber awareness and operational capability among maritime professionals. Its modularity allows it to be used by all classes of user, including deck officers, IT personnel, and shore-based managers, and both in training academies and on-board ships.

Looking forward, several areas are worth further investigation. First, there are metrics and performance measures with which to measure the effectiveness of maritime cybersecurity controls. Second, the integration of cybersecurity into existing maritime Safety Management Systems (SMS) merits further attention, so that cyber threats are given the same level of priority as physical safety risks. Third, future research needs to consider the interplay between new technologies, such as AI-based threat detection, autonomous ships, and maritime IoT and cybersecurity strategy and regulation. Besides, the CyberSEA consortium urges the establishment of a pan-European maritime cybersecurity knowledge-sharing network. This will enable operators, regulators, training organizations, and technology suppliers to exchange threat intelligence, share case studies, and collaborate to develop solutions fit for regional and operational contexts.

Overall, maritime cybersecurity is not a secondary issue but a cornerstone of safe and secure maritime operations in the era of digitization. The findings of this study uphold the call for an urgent, harmonized, cross-industry, and human-focused approach to cybersecurity planning in the maritime sector. As the dynamics of cyber threats evolve, so must the readiness of the industry, and that advancement must be supported by collaboration, innovation, and continued investment in systems and people. Enhancing maritime cybersecurity cannot be addressed in bits and pieces. This research supports that the maritime sector does not merely fall behind in having in place rudimentary cyber controls, but also in cultural and organizational maturity that other sectors such as finance, healthcare, and logistics enjoy. Filling these gaps requires concerted and sustained efforts over the long term on multiple fronts. Key results of the CyberSEA project confirm the need for:

- Cross-sectoral learning: Utilizing time-proven techniques from other sectors accelerates the development of relevant cyber strategies in the maritime industry.
- Continuing training and awareness: Cybersecurity should be prioritized in crew training and included in regular refresher training, simulated attacks, and onboarding processes for all personnel.
- Harmonised governance frameworks: Creating custom roles such as Maritime CISOs and delineating clear cyber roles will support decision-making and responsibility.
- Technology investment: Adoption of cost-effective, cloud-based security technologies like SIEM, IDS, and MFA can greatly improve early threat detection, including incident response capabilities.
- Regulatory enforcement: Enforcement of IMO's resolution MSC.428(98) and the incorporation of cyber risk management into the ISM Code is to be checked by port state control and flag state audits.

Through building a culture of cybersecurity by leveraging technology, governance, and training, the maritime industry can transform its weakest links into its greatest defences. Maritime cybersecurity cannot be enhanced by single-point solutions. To this end, an important contribution of this research is the proposal of a tailored maritime cybersecurity framework. By structuring the framework around governance, access control, data protection, training, and third-party risk management, it addresses the multifaceted nature of cyber threats. The inclusion of mobile device management (MDM) and BYOD policies also reflects emerging technological realities aboard vessels. However, the successful implementation of the proposed framework will depend on several enabling factors: cross-jurisdictional regulatory cooperation, investment in secure infrastructure, and stakeholder commitment to organizational change.

Acknowledgements: This research was supported by the European Union's Erasmus+ Programme under the project CyberSEA: Cyber Security in the European Maritime Sector (Project No. 2023-1-ES01-KA220-VET-000159793). The contents of this

publication reflect the views of the authors only, and the European Commission cannot be held responsible for any use that may be made of the information contained therein.

REFERENCES

BIMCO, 2021. *Cyber Security Guidelines for Ships*. 4th ed. Available at: https://www.bimco.org (accessed on: 01 June 2025).

Cariou, P., Mejia, M.Q. & Wolff, F.C., 2020. 'Shipboard cyber risk management: Analysis of IMO guidelines and industry practices', *Maritime Policy & Management*, 47(7), pp. 865–881. doi: 10.1080/03088839.2020.1761213

CyberKeel, 2020. *Maritime Cybersecurity Threat Analysis Report*. Available at: https://www.cyberkeel.com (accessed on: 5 June 2025).

DNV GL, 2016. *Maritime Cyber Safety – An Introduction to the Guidelines*. DNV GL Group.

Drewry, 2020. *Shipping and Trade Statistics*. Drewry Maritime Research.

EMSA, 2021. *Annual Overview of Marine Casualties and Incidents 2021*. European Maritime Safety Agency.

ENISA, 2021. *Cybersecurity for the Energy Sector*. European Union Agency for Cybersecurity.

ENISA, 2021. *Cybersecurity Guide for SMEs in the Financial Sector*. European Union Agency for Cybersecurity.

ENISA, 2022. *Cybersecurity for Ports and Maritime Organizations: Threat Landscape*. European Union Agency for Cybersecurity.

ENISA, 2022. *Threat Landscape for the Maritime Sector*. European Union Agency for Cybersecurity.

Erbas, M., Khalil, S. M., & Tsiopoulos, L., 2024. Systematic literature review of threat modeling and risk assessment in ship cybersecurity. Ocean Engineering, 306, 118059.

European Commission, 2016. *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)*.

European Commission, 2021. *Digital Europe Programme: Strategic Orientation 2021–2027*.

European Commission, 2022. *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*.

Greidanus, H. & van den Berg, P., 2018. 'The human factor in maritime cybersecurity: Policy implications', *Journal of Maritime Affairs*, 17(1), pp. 103–117. doi: 10.1007/s13437-018-00123-x

ICAO, 2021. *Manual on Cybersecurity in Civil Aviation (Doc 9985)*. International Civil Aviation Organization.

IMO, 2021. *Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3)*. International Maritime Organization.

ISO, 2013. *ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems – Requirements*. International Organization for Standardization.

Jones, K., Tam, K. & Papadaki, M., 2016. 'Threats and impacts in maritime cyber security', *Engineering & Technology Reference*, pp. 1–12.

Johnson, R. & Lee, A., 2019. 'Aging fleets and rising risks: Cybersecurity in older vessels', *Journal of Maritime Security*, 11(2), pp. 45–60. doi: 10.1007/s11617-019-01234-y

Katsikas, S.K., Lambrinoudakis, C. & Gritzalis, D., 2021. 'Cybersecurity in the maritime industry: A systematic review', *IEEE Transactions on Dependable and Secure Computing*, 18(4), pp. 1731–1746. doi: 10.1109/TDSC.2020.3021339

Kessler, G.C. & Craigen, D., 2016. 'Cybersecurity in the maritime domain', in Proceedings of the 2016 NATO Maritime Security Workshop.

Kessler, G.C. & Shepard, S., 2022. *Maritime Cybersecurity: A Guide for Leaders and Managers*. CRC Press. Available at: https://www.garykessler.net/MaritimeCybersecurity-Book (accessed on: 11 June 2025)

NIST, 2020. *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology.

Oruc, A., Kavallieratos, G., Gkioulos, V., & Katsikas, S., 2025. Perspectives on the Cybersecurity of the Integrated Navigation System. *Journal of Marine Science and Engineering*, 13(6), 1087. https://doi.org/10.3390/jmse13061087

Smith, R. & Taylor, D., 2021. 'Global logistics: Cyber threats in maritime supply chains', *Transport Security Journal*, 6(1), pp. 13–25. doi: 10.1007/s12345-021-00678-z

Tam, K. & Jones, K., 2018. 'Cyber-risk assessment for autonomous ships', in Proceedings of the 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Glasgow, 11–12 June 2018, pp. 1–8. doi: 10.1109/CyberSecPODS.2018.8560690

Tam, K. & Jones, K., 2019. 'MaCRA: A model-based framework for maritime cyber-risk assessment', *WMU Journal of Maritime Affairs*, 18(1), pp. 129–163. doi: 10.1007/s13437-019-00162-2

Vaarandi, R., Tsiopoulos, L., Visky, G., Rehman, M. U., & Bahşi, H., 2025. A Systematic Literature Review of Cyber Security Monitoring in Maritime. IEEE Access.