From the Baltic to the Mediterranean: A Comparative Review of Cloud-based Maritime Cybersecurity Strategies

Od Baltika do Sredozemlja: usporedna analiza pomorskih kibernetičkih strategija temeljenih na oblaku

Daisy Romanini*
a) Istituto di Informatica e Telematica CNR
Pisa, Italy
b) IMT Scuola Alti Studi Lucca, Italy
E-mail: daisy.romanini@iit.cnr.it

Esther Rodriguez
World Maritime University
Malmö, Sweden
E-mail: w1017946@wmu.se

Dimitrios Dalaklis
World Maritime University
Malmö, Sweden
E-mail: dd@wmu.se

Fabio Pinelli
IMT Scuola Alti Studi Lucca, Italy
E-mail: fabio.pinelli@imtlucca.it

Marinella Petrocchi
a) Istituto di Informatica e Telematica CNR
Pisa, Italy
b) IMT Scuola Alti Studi Lucca, Italy
E-mail: marinella.petrocchi@iit.cnr.it

DOI 10.17818/NM/2025/3.4
UDK 004:656.61(261.24)(262.3)
Review / *Pregledni rad*
Paper received / *Rukopis primljen:* 3. 9. 2025.
Paper accepted / *Rukopis prihvaćen:* 1. 12. 2025.

Abstract

This study provides a comparative review of how cloud integration is reshaping cybersecurity in the maritime sector, focusing on the Baltic and Mediterranean basins. It aims to identify how regional threat landscapes, governance frameworks, and industrial ecosystems influence both vulnerabilities and resilience in a sector increasingly reliant on digital infrastructures. Methodologically, the paper adopts a qualitative and interpretive approach, combining policy and regulatory analysis, technical assessment of OT/IT and cloud convergence, and case studies such as the NotPetya incident and the cybersecurity architecture of Fincantieri and its subsidiary E-phors. The paper contributes to the literature by (1) systematising regional approaches to maritime cyber resilience, (2) mapping transferable security patterns between two contrasting maritime ecosystems, and (3) integrating an industrial case study into a comparative governance framework. Theoretically, it extends maritime cybersecurity research by situating cloud adoption within regional security ecologies; practically, it highlights the managerial value of security-by-design practices, Zero Trust adoption, and cross-regional learning. Policy recommendations include the creation of EU-wide federated identity registries, regional threat intelligence hubs, and lifecycle-integrated cybersecurity frameworks across the maritime supply chain.

KEY WORDS

Maritime security
Cybersecurity
Cloud computing
Resilience
Governance
Zero Trust

Sažetak

Ovaj rad daje usporednu analizu načina na koji integracija oblaka mijenja kibernetičku sigurnost u pomorskom sektoru, s naglaskom na Baltički i Mediteranski bazen. Cilj je utvrditi kako regionalni profil prijetnji, upravljački okviri i industrijski ekosustavi utječu na ranjivosti i otpornost u sektoru koji je sve više ovisan o digitalnoj infrastrukturi. Metodološki, rad primjenjuje kvalitativni i interpretativni pristup, kombinirajući analizu politika i regulative, tehničku procjenu konvergencije OT/IT i oblaka te studije slučaja poput incidenta NotPetya, kao i kibernetičke arhitekture tvrtke Fincantieri i njezine podružnice E-phors. Rad doprinosi literaturi na tri načina: (1) sustavno prikazuje regionalne pristupe pomorskoj kibernetičkoj otpornosti, (2) identificira sigurnosne obrasce koji se mogu prenositi između različitih pomorskih ekosustava te (3) uključuje studije slučaja u komparativni okvir upravljanja. Na teorijskoj razini, proširuje istraživanja pomorske kibernetičke sigurnosti time što smješta usvajanje cloud tehnologija u kontekst regionalnih sigurnosnih ekologija. Na praktičnoj razini, ističe upravljačku vrijednost pristupa „sigurnosti po dizajnu", implementaciju Zero Trust modela i međuregionalnog učenja. Preporuke politike uključuju stvaranje registara identiteta na razini cijelog EU-a, regionalnih središta za razmjenu obavještajnih podataka o prijetnjama i okvira za kibernetičku sigurnost integriranih u životni ciklus u pomorskom lancu opskrbe.

KLJUČNE RIJEČI

pomorska sigurnost
kibernetička sigurnost
računarstvo u oblaku
otpornost
upravljanje
Zero Trust

1. INTRODUCTION / *Uvod*

In recent years, the maritime industry has come to recognise that cybersecurity resilience is no longer a peripheral concern, but a core element of maritime safety and operational continuity. As ports, shipping companies, and logistics chains undergo rapid digital transformation, the risk of cyberattacks has increased proportionally, exposing the industry to vulnerabilities that extend from critical infrastructures ashore to vessels at sea. While technological innovation (through automation, digital platforms, and advanced information systems) offers

* Corresponding author

significant potential to improve efficiency and sustainability, it simultaneously expands the attack surface and introduces new forms of risk. Within this evolving context, the human element has emerged as a decisive factor. Technology provides the tools for defence, but it is human awareness, decision-making, and competence that ultimately determine whether those tools are applied effectively.

The scale of this challenge is clearly reflected in recent statistics. A 2024 report by the European Maritime Safety Agency (EMSA) revealed that between 2014 and 2023, 58.4% of marine casualties were attributed to human actions, while 49.8% of contributing factors were linked to human behaviour. When these figures are considered together, they indicate that the human element was involved in more than 80% of all investigated marine casualties [1]. Although these metrics cover the broader spectrum of marine incidents and not exclusively those of a cyber nature, they underscore a crucial point: technology alone cannot guarantee resilience. Cybersecurity outcomes in the maritime industry depend as much on the awareness, vigilance, and competence of individuals (both at sea and ashore) as on the robustness of technical systems.

The persistence of human-centred vulnerabilities has also been documented at the national level. A 2021 study conducted in Greece revealed that even basic principles of information security and essential practices for protecting communication technologies from cyberattacks were not adequately understood within the country's maritime community [2]. This lack of awareness directly increases the exposure of maritime organisations to cyber risks, demonstrating the extent to which the human factor remains the weakest link in the cybersecurity chain.

Several concrete examples illustrate how such vulnerabilities materialise in practice. Weak password management, such as the use of easily guessed or frequently reused credentials, remains widespread. Inadequate authentication procedures, particularly the absence of multi-factor authentication (MFA), further diminish the reliability of access controls. Delayed software updates, often caused by limited awareness of patching requirements or fear of operational disruption, provide attackers with exploitable entry points into systems [3]. These weaknesses are not merely technical oversights, but evidence of a broader challenge: the difficulty of cultivating a culture of cybersecurity resilience within the maritime domain. In operational environments, lapses of this kind may allow intruders to gain unauthorised access to shared platforms, manipulate digital twin models, or compromise navigation and cargo-handling systems.

The persistence of such vulnerabilities points to a deeper structural gap: the mismatch between the pace of evolving cyber threats and the level of cybersecurity awareness and education among maritime professionals. This gap is widened by the rapid evolution of technology, which frequently outpaces training programmes and institutional responses. As cybersecurity becomes increasingly specialised, many academic programmes in maritime education remain misaligned with industry needs. As a result, graduates often enter the workforce with formal qualifications that fail to equip them with the skills required to manage real-world cyber risks [4]. This misalignment exacerbates the vulnerability of the sector and highlights the need for curricula and professional development initiatives that are more closely aligned with the realities of digital maritime operations.

Compounding this challenge is the global shortage of cybersecurity specialists. Even in well-resourced organisations, the demand for expertise consistently exceeds supply. A 2025 report by the World Economic Forum on the global cybersecurity workforce identified a deficit of over four million professionals worldwide, underscoring the structural lack of skilled expertise in the field [5]. For the maritime sector, this means that organisations cannot rely solely on the external labour market to fill their cybersecurity needs. Instead, they must invest in continuous training and upskilling of their existing workforce, ensuring that employees in diverse operational roles acquire the competencies necessary to address the growing cybersecurity demands of the industry.

Some progress has been made at the European level to address these gaps. In 2018, EMSA launched a short course on awareness in maritime cybersecurity [6]. Although introduced several years ago, the course was designed for periodic updates to reflect technological change. Beyond training, the EU has also supported capacity-building initiatives such as CyberMAR, a Horizon 2020 project implemented between 2019 and 2022. CyberMAR brought together stakeholders from the maritime industry, the cybersecurity sector, and academia (including the World Maritime University in Sweden) to address emerging cyber threats in maritime logistics. Its main contribution was the creation of a simulation environment capable of replicating real-world maritime systems such as ships, ports, and supply chains in a controlled setting. By enabling realistic simulations of cyberattack scenarios, the project allowed researchers and practitioners to assess vulnerabilities and test countermeasures [4]. CyberMAR not only highlighted the importance of technical defences, but also demonstrated how simulation-based education can strengthen awareness and preparedness among maritime professionals.

Against this backdrop, this paper examines how the integration of cloud technologies is reshaping cybersecurity practices in the maritime sector, with a comparative focus on the Baltic Sea and Mediterranean regions. Although both regions operate under common regulatory frameworks such as NIS2 and IMO guidance, their priorities, governance structures, and industrial ecosystems diverge markedly. The study employs a qualitative, comparative methodology that integrates regulatory and technical analysis with case-based insights; most notably the NotPetya incident affecting Maersk and the cybersecurity architecture developed by Fincantieri and its subsidiary E-phors.

The primary contribution of this paper is to offer the first empirically informed comparison of how different regional configurations (characterised by varying degrees of institutional coordination, industrial integration, and exposure to hybrid threats) shape the adoption of cloud-enabled maritime cybersecurity. The analysis identifies practices that are transferable across basins, outlines region-specific requirements, and formulates policy and managerial recommendations for strengthening cyber resilience through cloud governance and security-by-design approaches.

2. LITERATURE REVIEW / *Pregled literature*

The legal aphorism *ex facto oritur ius* ("law arises from facts") aptly illustrates how regulatory frameworks evolve in response to major disruptive events. In the maritime sector, the terrorist attacks of 9/11 exposed the limitations of traditional

security models focused solely on physical threats and led the International Maritime Organization (IMO) to adopt the International Ship and Port Facility Security (ISPS) Code [7, 8]. This regulatory milestone marked a shift from reactive to preventive security governance; an approach that is now being replicated in the digital domain.

Two decades later, the industry is experiencing a profound digital transformation driven by efficiency gains, cost reduction, and the growing demand for real-time data. However, this transformation introduces a new spectrum of vulnerabilities, as innovative technologies become potential vectors for cyber threats affecting safety and operations. Recent studies have underscored that digitalisation in the maritime domain creates both opportunities and dependencies. Dalaklis et al. [9] and Kitada et al. [10] highlight that increased automation and the adoption of Maritime Autonomous Surface Ships (MASS) have redefined operational safety and blurred the boundaries between IT and operational technology (OT) systems. These analyses collectively suggest that maritime cybersecurity must now be understood not as a standalone technical challenge, but as a systemic component of safety management.

Tonn et al. [11] conceptualise cyber-physical transport systems through a four-layered framework comprising:

I. the perceptual layer, where GPS and wireless sensors connect the physical and digital domains;
II. the network layer, which transmits data through satellite and internet infrastructures;
III. the computing layer, where cloud services and intelligent platforms operate; and
IV. the application layer, which interfaces directly with real-world maritime operations.

Modern vessels integrate all four layers, allowing adversaries to disrupt operations remotely; an asymmetry that magnifies risks to life and property at sea compared with pre-digital security incidents.

Within this structure, cloud computing (situated in the third layer) plays a pivotal role. Its service models (Software as a Service, Platform as a Service, and Infrastructure as a Service) are increasingly embedded in maritime processes. In practice, SaaS solutions support real-time cargo tracking and route optimisation, while IaaS architectures enable secure data storage, redundancy, and recovery through automated backup mechanisms. Industry reports and practitioner analyses highlight this shift, noting that while cloud adoption enhances efficiency, scalability, and cost-effectiveness, it also transfers critical data and control functions to third-party providers. This dependency introduces new layers of vulnerability, broadening the potential attack surface even as operational resilience improves [12].

The vulnerabilities inherent in such dependence have already been demonstrated in practice. The 2017 NotPetya incident that crippled Maersk's IT infrastructure caused losses estimated between USD 200 - 300 million, contributing to a USD 264 million quarterly deficit despite rising revenues. According to CEO Soeren Skou, the company avoided data breaches or data loss, a fortunate outcome given later analyses suggesting that NotPetya functioned more as a data-wiping weapon than as conventional ransomware [13]. Similarly, in the Black Sea, at least twenty ships reported falsified AIS positions appearing miles inland near a Russian airport, illustrating the dangers of signal spoofing and false situational awareness [14]. These incidents accelerated the institutionalisation of cyber resilience within maritime safety frameworks. In 2018, the IMO's Maritime Safety Committee (MSC) adopted Resolution MSC.428(98), mandating the integration of cybersecurity into Safety Management Systems (SMS) and formally linking cyber resilience to existing safety requirements.

This momentum continued in 2022, when the IMO's MSC and Facilitation Committee (FAL) jointly issued revised *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3/Rev.2). While non-binding, these guidelines provide high-level principles and recommended practices for cyber risk governance, encouraging member states and industry actors to develop structured management systems [15].

At the European level, regulation has evolved further. The NIS2 Directive (2022) extended the scope of the original NIS Directive to explicitly cover maritime operators, ports, and service providers[1]. It requires organisations employing cloud services in shipping operations to implement risk management, vulnerability assessment, and incident reporting mechanisms [16]. NIS2 also emphasises accountability at the governance level by assigning security responsibilities to company directors and introducing stronger enforcement measures. This reinforces the EU's broader strategy of embedding cybersecurity within critical infrastructure protection policies [17].

Alongside regulatory advances, a growing body of scholarship has examined the operational and managerial implications of digitalisation in maritime contexts. De Andres Gonzalez et al. [18] and Aro and Rytter [19] identify the Baltic Sea region as a frontrunner in adopting digital tools for port efficiency and environmental sustainability. By contrast, research focusing on the Mediterranean remains comparatively limited. Existing studies tend to address specific themes (such as cybersecurity awareness, maritime safety, or defence-oriented considerations), rather than providing a holistic assessment of digital transformation in the region. As a result, the Mediterranean's institutional diversity, its complex geopolitical environment, and its increasing reliance on cloud-based services remain underexplored in the academic literature.

In summary, existing research consistently recognises that while cloud technologies enhance operational efficiency, cost reduction, and data-driven decision-making, they also introduce new layers of complexity and risk [20]. What is missing is a systematic comparative analysis between the Baltic and Mediterranean regions, particularly with respect to the integration of cloud infrastructures, the governance of hybrid threats, and the organisational models through which cyber resilience is achieved. Addressing this gap is the primary motivation of the present study.

3. METHODOLOGY / *Metodologija*

This research adopts a qualitative, interpretive methodology to investigate how the integration of cloud technologies is reshaping cybersecurity practices in the maritime sector, with a comparative focus on the Baltic and Mediterranean regions. The analysis combines legal review, technical evaluation, and comparative policy analysis to uncover vulnerabilities, governance responses, and sector-specific dynamics. This framework reflects the inherently transnational character of maritime infrastructures, where cloud services, regulatory norms, and threat vectors intersect across regional and institutional boundaries.

[1] Directive (EU) 2022/2555. Article 6 (6).

To ensure depth and triangulation, the study draws on four categories of sources:

- Legal and regulatory frameworks: Reference is made to the NIS2 Directive, the ISPS Code, and the IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2), which collectively frame the standards and compliance obligations of maritime stakeholders. Their transposition and adaptation across regions serve as an indicator of institutional readiness and alignment.
- Operational case studies:
  - In the Baltic context, the 2017 NotPetya ransomware attack on Maersk serves as a key case study, demonstrating both the systemic vulnerabilities of digitalized operations and the cascading risks introduced by reliance on cloud-based infrastructures.
  - For the Mediterranean, the study incorporates the Fincantieri case, focusing on how a major European shipbuilder integrates cybersecurity by design in naval and cruise ship construction. This case demonstrates how industrial ecosystems in the Mediterranean, anchored in national champions, can embed security from the design phase, shaping end-to-end resilience patterns.
- Institutional and policy reports: Publications from ENISA, the European Commission, EMSA, and national cybersecurity authorities are considered to contextualize adoption trajectories, governance gaps, and regional coordination mechanisms.
- Academic and technical literature: Research on maritime digitalization, cyber-physical risks, and regional cooperation provides the conceptual foundation for this study.

4. E-NAVIGATION AND CLOUD IN THE BALTIC REGION / *E-navigacija i oblak u baltičkoj regiji*

As maritime operations become increasingly digital, regulatory compliance remains the foundation of lawful and safe conduct at sea. Frameworks such as the International Safety Management (ISM) Code, the Maritime Labour Convention (MLC), and evolving IMO environmental rules continue to shape global practices. By 2025, cloud-based compliance platforms have become critical enablers of these regimes, offering real-time regulatory updates, tamper-evident audit trails, and automated checklists that help operators meet obligations efficiently while reducing risks of penalties and operational delays [21].

A cornerstone of this transformation in the Baltic Sea is the Maritime Connectivity Platform (MCP), originally launched as the *Maritime Cloud* under the EU-funded EfficienSea2 programme, led by the Danish Maritime Authority (DMA). MCP provides a secure, service-oriented infrastructure for exchanging operational and navigational data across national boundaries. Its architecture combines a Service Registry (listing digital services such as route optimisation and weather feeds) and an Identity Registry (authenticating users and systems across jurisdictions) [22].

Introduced during the 2016 International e-Navigation Underway Conference, the platform was conceived as a unifying communication layer enhancing safety, security, and efficiency by bridging fragmented systems. DMA's Technology Director, Omar Frits Eriksson, framed MCP as a vehicle for "trustworthy interoperability". Since then, the platform has incorporated lessons from Sweden's STM Validation Project and South Korea's SMART Navigation initiative, refining its architecture and governance [23].

By 2025, MCP has evolved from concept to operational reality, supporting integrity, confidentiality, and authenticity for a broad range of maritime stakeholders. Its design aligns closely with NIS2 Directive requirements for risk management, periodic auditing, and incident reporting, especially for operators of critical maritime infrastructure [24].

Across the region, ports such as Hamburg, Gothenburg, and Gdańsk have implemented SaaS-based Port Community Systems (PCS) to streamline communications among customs, terminals, agents, and logistics providers. In Hamburg, the *Marketplace. Hamburg* platform integrates services for berth management, port fees, and truck scheduling, supported by partners such as HPA, DAKOSY, and HVCC. In early 2024, the Port of Gothenburg launched *Digital Port Call* (developed with Awake.AI) to enhance transparency, reduce vessel waiting times, and cut emissions [25, 26]. Similarly, the Port of Gdańsk adopted the Comarch ERP XL system to integrate accounting, HR, and document management within port operations [27]. Collectively, these initiatives show how cloud-based tools improve administrative coordination and turnaround efficiency [28].

To ground these developments, Table 1 summarizes the three principal cloud service models (SaaS, PaaS, and IaaS) along with their typical functions and representative maritime uses referenced throughout this section.

Despite these advances, digital maturity remains uneven. Ports in Germany, Denmark, and Sweden benefit from strong institutional capacity and advanced infrastructure, whereas smaller states such as Estonia and Latvia face funding and staffing constraints. This asymmetry creates cybersecurity weak points and complicates cross-border coordination. ENISA has flagged the lack of a harmonised cyber-risk assessment methodology across EU ports as a major obstacle to achieving a secure, integrated digital maritime ecosystem [24].

At the international level, IMO Secretary-General Kitack Lim has emphasised the need for harmonised data and interface standards, suggesting that the IMO may eventually take a broader role in governing digital maritime infrastructure. DMA Director General Andreas Nordseth complements this

Table 1 Cloud models in Maritime sector
Tablica 1. Modeli oblaka u pomorskom sektoru

Service model	Description	Examples in maritime use
SaaS *(Software as a Service)*	Cloud-based applications accessed via web interfaces	Ship tracking systems, Port Community Systems
PaaS *(Platform as a Service)*	Development platforms for building custom applications	Logistics scheduling platforms, digital twin modeling
IaaS *(Infrastructure as a Service)*	On-demand servers and storage	Vessel sensor data storage, cybersecurity backup systems

Source: Authors' elaboration based on [28]

perspective, arguing that digital transformation should balance regulation and market-driven innovation, ensuring that solutions remain responsive to user needs [29].

The Baltic experience demonstrates a high degree of institutional alignment and technical experimentation, yet it also exposes key deficiencies. The MCP and related initiatives have achieved interoperability and transparency, but governance fragmentation and uneven national implementation hinder full regional coherence. Moreover, many PCS deployments still depend on third-party cloud providers, raising questions of data sovereignty and jurisdictional accountability.

4.1. Threats to Maritime Cybersecurity / *Prijetnje pomorskoj kibernetičkoj sigurnosti*

While terrestrial networks have driven the rapid expansion of digital services, offshore systems lag behind due to bandwidth limitations and reliance on legacy radio technologies. The IMO's e-navigation initiative envisioned a suite of Maritime Services, but progress has been incremental. Experimental systems like the VHF Data Exchange System (VDES) and the TRI-Media Telematic Oceanographic Network (TRITON) remain constrained by performance barriers [30].

Within this environment, the shift toward cloud-based operations is reshaping the threat landscape. Cloud interconnectivity enhances efficiency and real-time coordination but simultaneously multiplies the potential attack surface. EMODnet partner surveys highlight concerns around data confidentiality, licensing, and jurisdictional ambiguity when working with non-EU providers. Respondents warned that "*data is like currency for research institutions… if abused or used without credit, it undermines the credibility of the work*" [28].

To mitigate these risks, the Blue-Cloud 2026 initiative extends the pilot Blue-Cloud architecture into a federated European data ecosystem. Rooted in FAIR data principles and aligned with the European Open Science Cloud (EOSC), it connects infrastructures such as EMODnet, Copernicus, SeaDataNet, and D4Science to ensure secure cross-border data access supporting EU Green Deal priorities [31].

Tonn's four-layer model [11] remains a useful analytical tool, mapping vulnerabilities across the maritime digital environment:

I. Perceptual layer: sensors, AIS, GPS, radars; threatened by spoofing and jamming.
II. Network layer: satellite and terrestrial links; exposed to denial-of-service and interception.
III. Cloud layer: storage and processing; at risk from misconfiguration, insider threats, and zero-day exploits.
IV. Application layer: user interfaces; vulnerable to phishing, credential theft, and malware.

This layered approach is visualized in Figure 1, which outlines the cyber-attack surface of maritime cloud systems, mapping vectors such as phishing, malware, and network compromise against core elements including port platforms, vessel systems, logistics networks, and sensitive data repositories. By overlaying these risks onto SaaS, PaaS, and IaaS models, the figure underscores the deeply interconnected nature of maritime digital infrastructures.

Historical precedents illustrate the stakes. The NotPetya ransomware incident disrupted operations in Gdańsk and Gothenburg, with losses exceeding USD 250 million. Recurrent GPS spoofing incidents in the Black Sea have raised similar

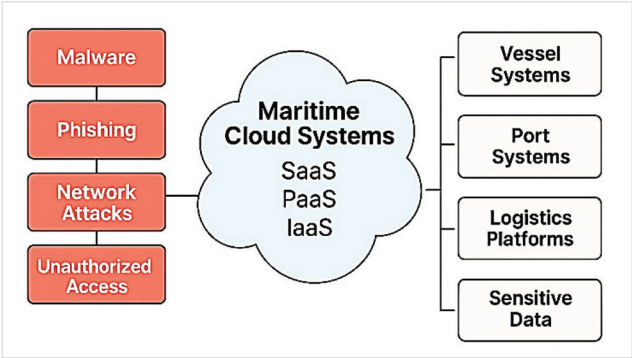

Figure 1 Cyber-attack surface in Maritime Cloud systems
Slika 1. Površina kibernetičkog napada u pomorskom sustavu oblaka
Source: Authors' elaboration based on [11]

alarms for the Baltic corridor. [11, 14].

Persistent use of legacy SCADA systems lacking segmentation and secure patching amplifies these vulnerabilities [24]. Moreover, weak password discipline, inadequate multi-factor authentication, and insecure "bring-your-own-device" practices continue to undermine resilience [15].

Finally, contractual ambiguities within Service Level Agreements (SLAs) add another layer of exposure. When cloud providers operate outside EU jurisdictions, issues of accountability, breach notification, and liability remain largely unresolved [32].

4.2. Regional Coordinatıon and Policy Gaps / *Regionalna koordinacija i nedostaci u politikama*

Technical vulnerabilities in maritime cloud systems reveal deeper governance challenges. Although the NIS2 Directive establishes a common EU baseline, its implementation across the Baltic remains fragmented. States such as Sweden and Germany have mature maritime cyber units, while others lag behind in incident response capacity [32]. The absence of a real-time threat intelligence sharing mechanism further weakens collective resilience: national CERTs operate largely in isolation, with voluntary information exchange and inconsistent data formats [24]. International guidelines, such as the IMO's MSC-FAL.1/Circ.3/Rev.2, provide a baseline but remain non-binding, leading to patchy uptake across the region [15].

A recent text mining review of 155 maritime sustainability studies confirms this gap: while research has extensively addressed emissions, port sustainability, and regulatory compliance, cybersecurity and digital integration remain underexplored, especially in the context of regional cooperation. Nonetheless, two Baltic digitalisation pilot projects, such as the Maritime Connectivity Platform (MCP) and the Sea Traffic Management (STM) system (in the Ports of Rauma and Gävle), demonstrate the benefits of coordinated data sharing. By enabling real-time updates and shared intentions among port actors, these pilots achieved more predictable operations, reduced delays, and improved transport efficiency. These results offer scalable models for broader application across the Baltic and beyond, with added environmental and logistical advantages. MCP focuses on secure, standardised communication and identity management, while STM supports operational optimisation through shared voyage plans and port-call coordination. Together, these systems illustrate two complementary approaches to maritime digitalisation: one

Table 2 Comparative Functional focus of MCP vs. STM
Tablica 2. Usporedni funkcionalni fokus MCP-a i STM-a

Dimension	Maritime Connectivity Platform (MCP)	Sea Traffic Management (STM)
Type	Communication and identity infrastructure	Operational coordination and situational awareness system
Core Functions	- Identity Registry - Service Registry - Secure message exchange	- Real-time voyage plan sharing - Port call synchronization - Enhanced navigational efficiency
Strengths	- Cross-border interoperability - Open-standard architecture - Strong alignment with NIS2 requirements	- Demonstrated reductions in delays, fuel burn, and emissions - Strong operational value for ports and vessels - High compatibility with digital-port-call initiatives
Weaknesses	- Adoption remains uneven (strong in Denmark/Sweden; weaker elsewhere) - Requires long-term governance beyond project-driven funding - Limited operational uptake by smaller Baltic ports	- Limited geographic deployment (Rauma, Gävle, and selected pilots) - Requires significant integration effort for new participants - No formal regional authority ensures long-term maintenance

Source: Authors' elaboration based on [18, 22, 23, 24]

governance-driven (MCP), the other operational-performance-oriented (STM) [18, 22].

Table 2 provides a structured comparison of the two systems, highlighting their respective strengths, limitations, and potential for wider regional deployment.

Despite the promise of such systems, their adoption has been hindered by institutional, regulatory, and technical constraints. While maritime industry stakeholders recognize the importance of data sharing (particularly algorithms and predictive models) they emphasize that meaningful transparency requires robust legal protections. Without binding regulations or incentives, many actors remain reluctant to disclose data due to concerns over competitive advantage. In addition, high integration costs, incompatible digital systems, and lack of common technical standards remain major barriers. Although optimism around digital transformation exists, real progress will depend on sustained investment and policy alignment [19].

Strategically, the creation of a public-private partnership for near-real-time cyber threat indicator sharing could enhance regional resilience. BIMCO has been suggested as a potential coordination hub to bridge communication between private maritime stakeholders and public cybersecurity authorities. Given the region's geopolitical vulnerability (particularly amid tensions with Russia) proposals have also emerged to establish a dedicated Baltic Sea Hybrid Threats Fusion Cell. Modeled after the EU INTCEN Hybrid Fusion Cell, such an initiative could provide strategic threat analysis, coordinate early warning efforts, and serve as a liaison with NATO and EU institutions. This would help restore lost analytical capabilities and improve the region's collective cyber defense posture [19, 33].

The Baltic Sea's economic and strategic significance further underscores the urgency of coordinated action. With over 881 million tons of cargo handled and approximately 40 million ferry passengers annually, and nearly 2,000 vessels operating in the region at any given time, the Baltic is one of the busiest maritime corridors in the world [34]. Economic analyses indicate that maritime digital communications revenues closely track global fleet size (driven by both new shipbuilding and retrofits), which supports KPMG's conclusion that connectivity is becoming a core component of fleet investment decisions. Still, these decisions are shaped not just by operational benefits but also by the stability of regulatory environments and broader trade dynamics [34].

Finally, legal and financial uncertainties continue to undermine confidence in cloud adoption. Maritime insurance rarely provides clear coverage for cloud-related cyber incidents, particularly those involving third-party providers. Liability questions, who is responsible after a breach and how compensation is secured, remain unresolved. Without enforceable legal frameworks to clarify accountability, operators may remain hesitant to fully integrate cloud services into critical operations [14].

In summary, the Baltic region exemplifies both progress and paradox: high digital ambition paired with uneven implementation and governance fragmentation. Its open, interoperable systems showcase a model of innovation-driven integration, but also expose critical coordination and liability gaps. This mixed performance provides a valuable benchmark for comparison with Mediterranean approaches, where cyber resilience is increasingly pursued through vertically integrated governance and internalized control mechanisms.

5. MEDITERRANEAN CLOUD-ENABLED MARITIME SECURITY / *Oblaci kao temelj pomorske sigurnosti u Mediteranu*

The Baltic Sea case illustrated how a relatively compact and cooperative region can lead the way in digital transformation and maritime cybersecurity governance. Shared regulatory alignment, harmonized technological standards, and coordinated initiatives (such as cloud-based communication platforms) have proven to enhance resilience and trust among maritime stakeholders [17, 35].

By contrast, the Mediterranean basin presents a more fragmented yet industrially dynamic environment, where cloud integration and cybersecurity governance evolve under geopolitical tension and uneven institutional capacity. While it is one of the world's busiest maritime corridors, handling vast flows of commercial cargo and dense passenger traffic [36], its cybersecurity environment is shaped by distinct challenges. Geopolitical volatility linked to North Africa, the Middle East, and Southern Europe, coupled with diverse institutional capacities across littoral states, has produced an environment where cloud adoption, OT/IT integration, and critical infrastructure protection follow different priorities than in the Baltic.

Within this setting, the industrial and technological role of Fincantieri, one of the world's leading shipbuilders, offers a valuable case study. Through its dedicated cybersecurity branch, E-phors, Fincantieri has pioneered new approaches to securing maritime operations against digital threats. Its initiatives illustrate how Mediterranean industry leaders are operationalizing cyber resilience through vertically integrated, security-by-design frameworks. This model contrasts with the Baltic's multi-actor openness: where northern Europe emphasizes cross-border interoperability, the Mediterranean demonstrates an inward, enterprise-centric approach that fuses cybersecurity with industrial strategy.

5.1. Overview of the Mediterranean Cybersecurity Landscape / *Pregled stanja kibernetičke sigurnosti u Mediteranu*

The Mediterranean maritime space embodies a unique combination of operational intensity and geopolitical complexity that directly shapes its cybersecurity posture. Unlike the relatively compact and coordinated Baltic basin, the Mediterranean functions as a vast crossroads of continents, trade routes, and political systems. It hosts high volumes of containerized trade, roll-on/roll-off (ro-ro) traffic, energy logistics, and cruise tourism, while also accommodating dense passenger flows and migration across its southern and eastern approaches. Ro-ro vessels (defined under the SOLAS Convention as passenger ships with cargo spaces for vehicles) are a cornerstone of short-sea routes. The global ferry industry is comparable in size to the commercial airline sector, carrying more than four billion passengers and hundreds of millions of vehicles annually. Yet this prominence has also been marked by serious safety incidents, including the capsizing of the *Herald of Free Enterprise* in 1987 and the sinking of the *Estonia* in 1994. Its exposure to two of the world's most critical chokepoints, the Suez Canal and the Strait of Gibraltar, amplifies the strategic consequences of disruption: even localized cyber incidents can ripple through global supply chains [37, 38].

Digital transformation in the Mediterranean follows similar trajectories to those observed elsewhere in Europe, but under more fragmented conditions. Port Community Systems (PCS) have become pivotal digital platforms, connecting the diverse organizations that make up seaport communities and enabling secure information exchange that optimises and automates logistics processes. Closely linked are Maritime Single Windows (MSW), which extend PCS integration to national and international levels, reducing duplication of reporting and ensuring compliance with European directives on maritime digitalisation. Together, PCS and MSW underpin more transparent, harmonised, and competitive supply chains. Increasingly, these solutions are complemented by digital customs platforms, predictive logistics tools, digital twins of terminals, remote pilotage support, and AI-driven maintenance scheduling. Most are deployed across SaaS, IaaS, and PaaS cloud models, which enhance efficiency and situational awareness, but also broaden the attack surface and deepen dependencies on multi-cloud infrastructures and third-party providers [37].

Regulatory alignment exists at the European level, but its application in the Mediterranean reflects considerable institutional diversity. The NIS2 Directive (Directive (EU) 2022/2555), IMO guidelines on cyber risk management (MSC-FAL.1/Circ.3/Rev.2), and industry-driven standards such as the BIMCO/ICS guidelines provide the overarching framework. Yet implementation varies: agencies like Italy's ACN, France's ANSSI, Spain's INCIBE, Greece's NCSA, and Malta's cyber authorities adopt divergent models of coordination with maritime regulators and coast guards. Some emphasize military and defense-industrial integration; others prioritize civilian crisis management or law-enforcement liaison. The result is uneven cyber preparedness across the region's ports and shipping operators [15, 38, 39, 40, 41].

The Mediterranean threat landscape can be summarized across three dimensions:

1. Cloud attack surface expansion
   Cruise lines, Ro-Ro operators, and LNG (liquefied natural gas) logistics rely heavily on cloud-based systems. SaaS-based PCS, IaaS for telemetry, and PaaS for AI/ML optimization are now standard. Hybrid and multi-cloud deployments balance cost and sovereignty but introduce vulnerabilities around provider responsibility, federated identity, and supply chain resilience [42, 43].
2. Operational stress on OT/IT integration
   Mediterranean ports combine legacy Operational Technology (OT), such as Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) systems, with modern IT tools; including Security Information and Event Management (SIEM) platforms, Identity and Access Management (IAM) solutions, and endpoint security. Seasonal traffic peaks and external disruptions strain these environments, while weak segmentation, irregular patching, and poor identity proofing create entry points for attackers [44].
3. Hybrid activity shaped by geopolitics
   Located at the intersection of volatile theaters, the region faces GPS spoofing, AIS (automatic identification system) manipulation, and disinformation. Even small-scale ransomware incidents can gain strategic weight amid political tensions or migration crises. Sensitive SAR (Search and Rescue) and law-enforcement data further complicate privacy and compliance [45].

Incident response requires multi-agency integration involving CSIRTs, port authorities, customs, and coast guards, aligned with NIS2 obligations [24]. Capability gaps remain; large hubs like Trieste [46], Genoa [47], Marseille-Fos [48, 49], Valencia [50], and Piraeus [51] maintain SOCs and cyber-ranges, while smaller ports depend on generic outsourced services, limiting contextual adaptation. Unlike the Baltic, Mediterranean exposure to geopolitical shocks and reliance on cruise/passenger flows heighten the stakes, demanding tighter links between cybersecurity, crisis communication, and public-order management [52].

5.2. The Fincantieri Approach: E-phors / *Fincantieri pristup: E-phors*

Fincantieri represents one of the most significant actors in global shipbuilding, with a portfolio spanning naval platforms, cruise vessels, critical infrastructure, and advanced integrated systems. The company's position, as both a leading industrial enterprise and a strategic defense supplier (contributing approximately

1% of Italy's GDP), renders cybersecurity not merely a technical concern, but a matter of national and international security [53]. Through E-phors, a spin-off from its internal cyber division, Fincantieri demonstrates how industrial actors can institutionalize cyber governance and export it as a service.

As observed by Stefano Landucci, Head of Head of Presales and Cybersecurity Solutions at Fincantieri/E-phors, the company's cybersecurity strategy is shaped by a dual imperative: "*protecting the internal corporate network and shipyard OT, while ensuring product-level resilience in external markets. It is not a support function, but a capability embedded into design, integration, and service delivery*".

The establishment of E-phors, originally derived from the Group's internal cybersecurity division, institutionalised this model. Conceived as a dedicated centre of excellence, E-phors consolidates governance across Fincantieri while simultaneously delivering advanced services to external stakeholders, including naval defence customers and commercial cruise operators [54]. Landucci notes that the subsidiary thus plays a dual role: internally safeguarding the Group's industrial backbone, while externally providing tailored services (such as red teaming, SOC transfer, and architecture reviews), addressing the specific threats of the maritime domain.

This comprehensive approach can be better understood across several key dimensions, which together illustrate how Fincantieri and E-phors embed cybersecurity throughout their operations and products:

- **Governance and frameworks**

The governance model adopted by E-phors reflects a centralized structure designed to ensure consistency across a diversified enterprise ecosystem of shipyards, subsidiaries, and supply chains. It is aligned with international standards such as ISO/IEC 27001, Italy's National Cybersecurity Perimeter (PSNC) [55], and the EU NIS2 Directive, thereby embedding resilience into assets classified as critical infrastructure. The architectural baseline is defined by Zero Trust, a security philosophy built on three core principles: verify explicitly, enforce least-privilege access, and assume breach. Rather than trusting anything inside the corporate perimeter, Zero Trust treats every access request as potentially hostile, requiring continuous authentication, granular access controls (e.g., JIT/JEA), and strict network segmentation. This shift from a "trust-by-default" to a "trust-by-exception" model reduces attack surfaces, improves detection, and enhances resilience across users, devices, applications, and data, regardless of location policies [56].

Operational capacity is concentrated in a Group-wide Security Operations Center (SOC) that integrates advanced tools, including Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms, Extended Detection and Response (XDR), Network Access Control (NAC), Data Loss Prevention (DLP), and real-time threat intelligence feeds. This configuration facilitates both proactive threat hunting and rapid incident response across geographically distributed infrastructures.

- **Securing shipyards and vessels**

Fincantieri's shipyards constitute highly heterogeneous environments, where legacy OT coexists with digitalized production technologies such as SCADA, robotics, and digital twins. These settings present significant cyber risk, as disruptions can entail cascading effects on production continuity and worker safety. Landucci has underlined that a successful cyberattack in such contexts could not only cause significant financial damage, but also lead to production delays and even risks to worker safety. To address this, E-phors enforces strict IT/OT segregation, industrial demilitarized zones (DMZs), and privileged access management (PAM) for remote interventions [57].

The same philosophy is extended to vessel-level design. Reference architectures developed by E-phors adopt ISA/IEC 62443 zoning principles, a globally recognised set of standards for securing Industrial Automation and Control Systems (IACS). These standards define best practices and performance benchmarks, taking a holistic approach that integrates operational and information technologies while aligning process safety with cyber protection. Widely applied across multiple sectors (from energy and transportation to manufacturing and medical devices), they serve as a key reference for assessing and improving industrial cybersecurity [58]. Unidirectional gateways and intrusion detection tailored to maritime OT environments further ensure that safety-critical systems, such as navigation and propulsion, remain isolated from business IT, while still allowing for secure integration of cloud-based analytics and remote support functions [59].

- **Product-level cybersecurity**

Given the long operational lifecycle of naval platforms, vulnerabilities introduced at the design or integration stage can create persistent liabilities. E-phors therefore applies cybersecurity-by-design, embedding secure development practices, SBOM (Software Bill of Materials) management, and staged software rollouts with cryptographic verification.

Recognizing the limited availability of specialized cybersecurity expertise onboard ships, E-phors has also developed an AI-driven monitoring and decision-support system (DSS) tailored to maritime crews. The solution provides real-time visibility into incidents and translates threat intelligence into actionable remediation steps. Landucci stresses that "*we cannot expect every vessel to have cyber specialists on board. Our cockpit interface allows crews to see exactly where an incident occurs, what it affects, and what steps to take, reducing both response time and human error*". At scale, this capability integrates AIS data, onboard telemetry, and threat intelligence feeds into a unified monitoring framework covering entire fleets.

The practical implementation of this architecture is supported by the *Maritime GUI* (Graphical User Interface), which provides crews with a user-friendly interface for situational awareness (Figure 2) and structured incident response workflows (Figure 3). These tools translate complex technical events into clear visualizations and guided actions, enabling non-specialist personnel to react effectively under cyber stress.

- **Strategic vision**

As part of its broader digital transformation strategy, Fincantieri has developed *Navis Sapiens*, an advanced maritime platform designed to accelerate the digitalisation of naval assets and operations. This initiative reflects a wider shift toward smart, connected vessels capable of real-time data exchange, predictive maintenance, and fully integrated lifecycle management.

At the core of Navis Sapiens lies a dual architecture that combines an onboard intelligence layer with a cloud-based digital twin. This configuration enables continuous interaction between ships, shipyards, and cloud services, supporting data-driven decision-making and enhancing operational coordination

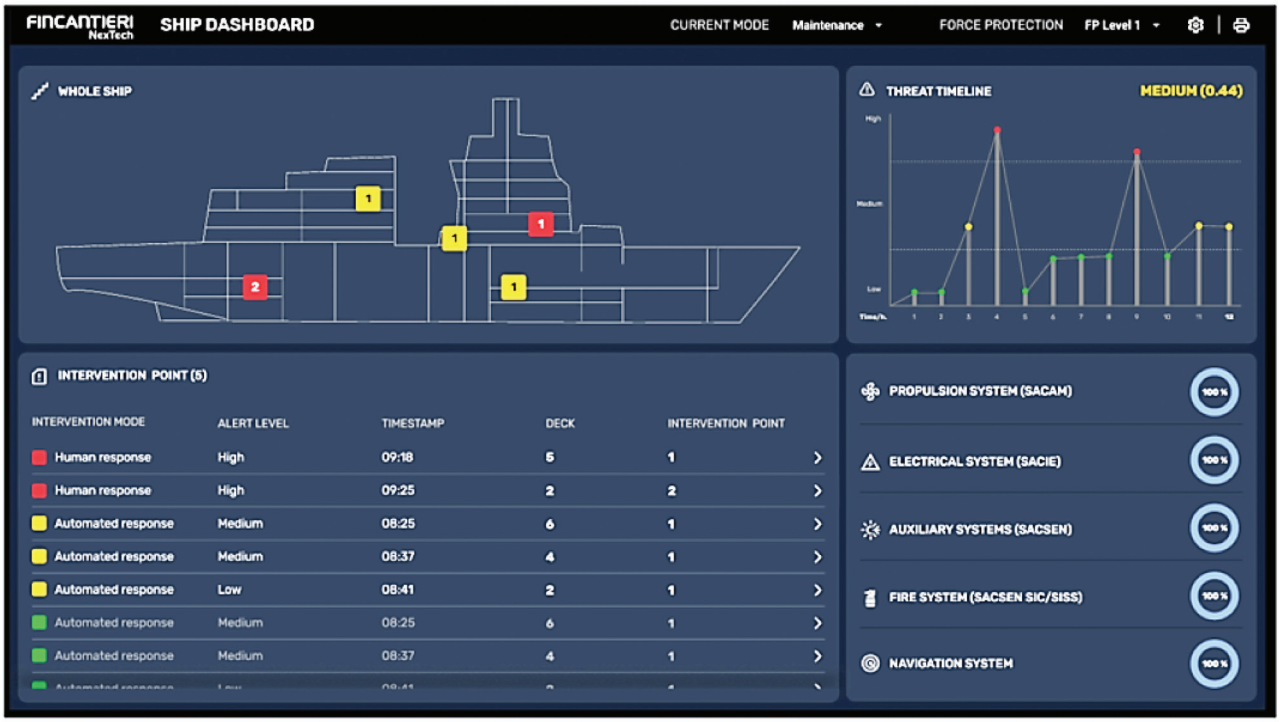

Figure 2 View of the Maritime GUI - Home dashboard

Slika 2. Prikaz korisničkog sučelja pomorskog sustava – početna nadzorna ploča

Source: *Maritime Cyber Security Platform (MCSP)* [59]

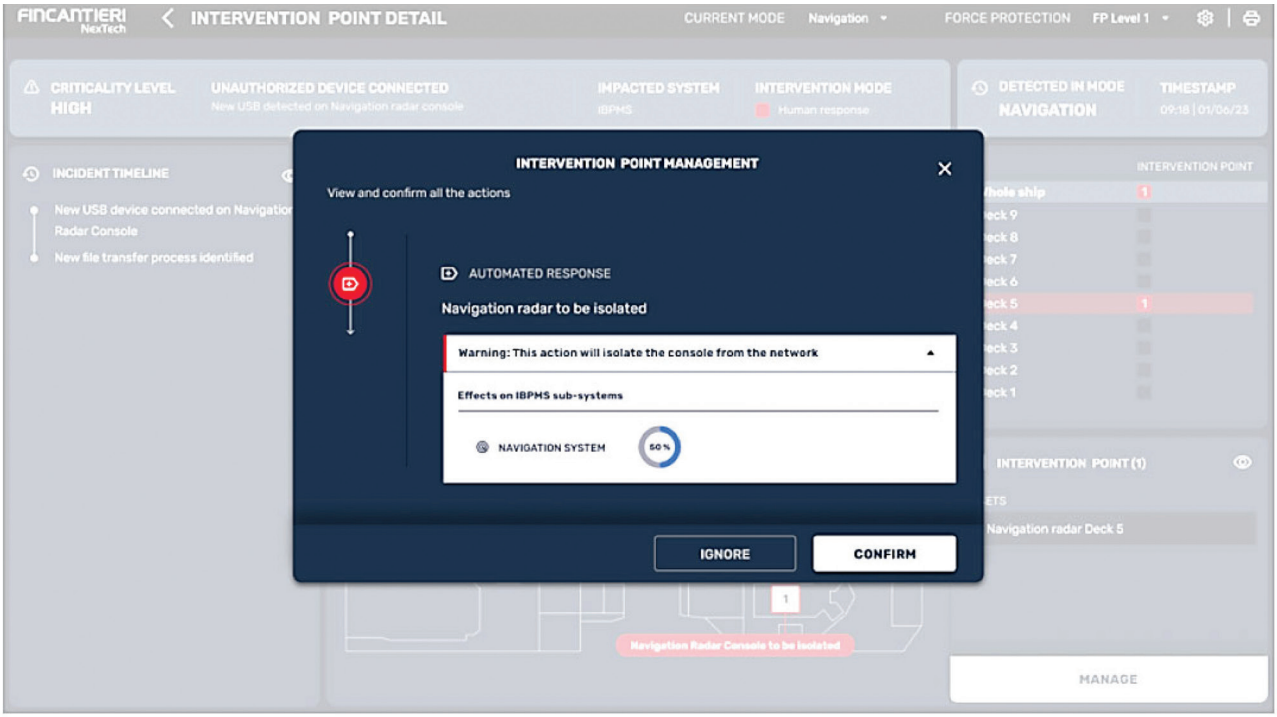

Figure 3 View of the Maritime GUI - Incident management module

Slika 3. Prikaz korisničkog sučelja pomorskog sustava – modul za upravljanje incidentima

Source: *Maritime Cyber Security Platform (MCSP)* [59]

throughout the vessel's lifecycle. To secure such a highly connected ecosystem, E-phors has embedded security-by-design principles into the platform's architecture from the outset. This includes the deployment of next-generation firewalls (NGFW), SD-WAN and SASE frameworks, intrusion detection and prevention systems (IDS/IPS), container security, operating-system hardening, API protection mechanisms, web application firewalls (WAF), and DevSecOps workflows to ensure ongoing software integrity.

Data protection forms a central pillar of the architecture. Safeguards include encryption at rest and in transit, granular access controls, data masking and anonymisation, and data loss prevention (DLP). These are complemented by robust identity and access management (IAM), multi-factor authentication (MFA), privileged access management (PAM), and secure cryptographic key and certificate lifecycle management. All components of the ecosystem are continuously monitored through a combination of

third-party cybersecurity technologies and E-phors' proprietary maritime cybersecurity platform, which provides real-time visibility, threat detection, and guided incident response across both onboard and cloud environments.

To maintain proactive defence, Navis Sapiens incorporates dynamic application security testing (DAST), vulnerability management, and structured patching processes. The platform also supports secure shipyard-to-vessel connectivity and controlled access to a service marketplace, facilitating new digital operating models while maintaining high levels of cyber resilience. Navis Sapiens is expected to become operational by the end of 2025, representing a major milestone in the secure digitalisation of maritime assets [60].

While E-phors exemplifies best practice in embedding cybersecurity into shipbuilding, it also reveals structural limitations. Its centralised, proprietary model ensures depth and control, but may reduce interoperability with smaller suppliers and external systems. Strong reliance on internal governance can constrain transparency and cross-regional data exchange; areas that Baltic frameworks explicitly address through open-standard architectures such as the Maritime Connectivity Platform (MCP). Moreover, the cost and complexity of implementing Fincantieri-level cybersecurity may limit scalability for mid-sized Mediterranean shipyards.

In comparative perspective, the Mediterranean model reflects resilience through vertical integration and sovereign control, whereas the Baltic emphasises resilience through distributed coordination. Each approach carries trade-offs: the Baltic risks fragmentation; the Mediterranean, over-centralisation. Recognising these complementary strengths and weaknesses provides a foundation for developing balanced, interoperable, and scalable maritime-cybersecurity strategies across Europe.

6. COMPARATIVE ANALYSIS: BALTIC VS. MEDITERRANEAN PRACTICES */ Usporedna analiza: prakse u Baltiku i Mediteranu*

The comparative assessment of the Baltic and Mediterranean basins highlights how distinct geopolitical, institutional, and industrial constellations shape the adoption of cloud-enabled maritime cybersecurity. While both regions operate under common regulatory frameworks such as the EU NIS2 Directive and IMO cyber risk management guidelines, their practices and priorities diverge in meaningful ways:

- **Threat models**

The Baltic Sea, though geopolitically exposed to Russian hybrid tactics, presents a relatively compact and cooperative environment where cross-border logistics and critical infrastructure form the main targets [61]. By contrast, the Mediterranean combines state-linked threats with highly specific challenges such as protecting passenger privacy in the cruise industry, securing Search and Rescue (SAR) operations, and managing risks linked to the Suez Canal as a global chokepoint. In this sense, the Mediterranean threat model integrates humanitarian, commercial, and supply-chain dimensions more directly than the Baltic.

- **Institutional constellations**

Institutional landscapes differ significantly. In the Baltic, regional pilots such as Sea Traffic Management (STM) have fostered a culture of interoperability and civilian cross-border coordination. Nordic states, accustomed to cooperative governance, leverage such pilots to harmonize standards and strengthen joint crisis response [35, 41]. In contrast, Mediterranean cooperation is more nationally anchored, with large hubs such as Genoa, Marseille, and Piraeus driving cybersecurity policies [47, 48, 51]. National defense-industrial ecosystems and law-enforcement agencies (e.g., coast guards and cybercrime units) play a central role in maritime incident management, reflecting a more securitized governance model [40, 55, 62].

- **Industry partnerships**

Industry partnerships also follow different trajectories. Baltic innovations have been driven by publicly funded EU projects such as the Maritime Connectivity Platform (MCP) and STM, with academia and regulators as key conveners (DMA/EfficienSea2, 2016 - 2018) [22]. The Mediterranean, on the other hand, emphasizes industrial champions (particularly shipbuilders and defense integrators like Fincantieri and its cybersecurity arm E-phors) who embed "security by design" directly into vessel architecture, supply chains, and port operations [36]. This model achieves depth and control but may limit transparency and interoperability with smaller suppliers.

- **Control baselines and transferability**

Despite these divergences, control baselines are converging. Both regions prioritize OT/IT segmentation, Zero Trust identity management, secure vendor access, and role-based workforce training. Yet Mediterranean practices show greater integration of Security Operations Centers (SOCs) with law-enforcement liaison, as well as stronger emphasis on privacy-preserving analytics due to cruise and passenger operations. Conversely, the Baltic provides a blueprint for federated identity and service registries (MCP-inspired), which could reduce duplicated integration costs in Mediterranean hubs [22, 23, 24].

The following cross-walk Table 3 summarizes the comparative emphases of the Baltic and Mediterranean regions. It highlights the main thematic areas where practices converge or diverge, and points to transferable actions that could enhance resilience, if adapted across both maritime basins (particularly in cloud governance, OT/IT segmentation, and workforce training).

Table 3 Baltic vs. Mediterranean maritime-cybersecurity Ecosystems
Tablica 3. Kibernetičko-sigurnosni ekosustavi u pomorstvu: Baltik naspram Mediterana

Dimension	Baltic Practices	Mediterranean Practices	Transferable Insights
Governance	Cooperative, cross-border (STM, MCP)	Nationally driven, defense-industrial (Fincantieri / E-phors)	Combine regional coordination with sovereign control
Cloud focus	Federated identity, open standards	Vertically integrated, security-by-design	Harmonize interoperability and supply-chain assurance
Threat model	Hybrid interference, logistics disruption	Multi-vector: data, SAR, passenger, chokepoints	Develop adaptive, scenario-specific exercises
Institutional capacity	Even regulatory maturity	Uneven across states	EU-level benchmarking and shared training
Industry role	Public-academic pilots	Industrial champions	Cross-basin innovation partnerships

Source: Authors' elaboration based on [22, 23, 23, 35, 36, 40, 41, 55, 61]

7. OBSERVATIONS AND CONCLUSIONS / *Zapažanja i zaključci*

The findings indicate that while both the Baltic and Mediterranean have internalized the inevitability of cyber risk in cloud-enabled ecosystems, they embody complementary philosophies of resilience:

- the Baltic model: federated, interoperable, and regulation-driven;
- the Mediterranean model: centralized, industrial, and design-integrated.

These contrasts highlight that effective maritime-cybersecurity strategy cannot rely on a single template, but must adapt to regional operational realities.

However, the research also identifies several deficiencies. The Baltic's heavy dependence on EU-project funding and voluntary information-sharing may hinder long-term sustainability once pilot programs end. The Mediterranean's enterprise-centric security architecture, while robust internally, risks reduced transparency and interoperability for smaller partners. Bridging these weaknesses requires hybrid governance models that combine distributed coordination with industrial accountability.

Looking ahead, several policy implications stand out for EU maritime governance as a whole:

1. Establish an *EU Maritime Cyber Resilience Program* that aligns regional pilots (e.g., STM in the Baltic) with industrial champions (e.g., Fincantieri-led programs in the Mediterranean). This would accelerate the mainstreaming of security-by-design while ensuring interoperability across basins.
2. Create a *cross-basin maritime cyber fusion cell* under ENISA and EMSA to integrate cyber threat intelligence, incident reporting, and early warning. Its remit should explicitly include hybrid threats linked to logistics disruption, disinformation, and passenger privacy breaches.
3. Develop an *EU-level certification for maritime cloud services*, combining MCP-inspired registries with sovereignty-aware safeguards. Such a framework would reduce duplicated integration costs for operators and enhance trust in multi-cloud deployments.
4. Invest in *workforce pipelines* that bridge operational and cyber domains. Joint academies, role-based certifications, and port authority-university partnerships should ensure that OT engineers, coast guards, and SOC analysts develop common vocabularies and response habits.
5. Future academic research should model cross-regional interoperability through *quantitative simulations or scenario-based stress tests* and evaluate cost-benefit dynamics of federated versus centralized cyber-resilience architectures.

Ultimately, the comparative analysis demonstrates that neither region provides a complete template for maritime cyber resilience. The Baltic's collaborative governance and the Mediterranean's industrial security-by-design represent complementary strategies that, when synthesized, could form the foundation for an integrated *European Maritime Cybersecurity Framework*. Leveraging both models would allow Europe to lead globally in securing cloud-enabled maritime operations, ensuring that digital transformation enhances, rather than endangers, the safety and sustainability of the seas.

Author Contributions: Conceptualization, Investigation, Writing - Original Draft, D. R.; Investigation, Writing - Original Draft, E. R.; Supervision, Writing - Review & Editing, D. D.; Supervision, Writing - Review & Editing, F. P., Conceptualization, Supervision, Writing - Review & Editing, M. P.

Funding: This work was partially supported by project SERICS [PE00000014] under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU; and by project EMERALD (Evidence Management for Continuous Certification as a Service in the Cloud) under the Horizon Europe program funded by the European Union [grant agreement No. 101120688]. Part of the activities described in this manuscript have been developed within Fincantieri's project "Connect 2 the Future", funded by the European Union - NextGenerationEU as part of IPCEI - CIS [CUP: B99J24001080005].

Conflicts of Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

Acknowledgements: The authors wish to thank Stefano Landucci (Head of Presales and Cybersecurity Solutions), Valentina Zuiani (Cybersecurity Communication Designer) and Giuseppe Laurenza (Maritime R&D Engineer) for their contribution to the development of the Fincantieri/E-phors case study presented in this manuscript.

Acknowledgement of AI or AI-assisted tools use: During the preparation of this work the authors used ChatGPT-5 for grammar and spelling checking. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the published manuscript.

REFERENCES / *Literatura*

[1] European Maritime Safety Agency (2024, November 20). Annual overview of marine casualties and incidents 2024. Retrieved from: https://www.emsa.europa.eu/publications/reports/item/5352-annual-overview-of-marine-casualties-and-incidents-2024.html

[2] Pseftelis, T. & Chondrokoukis, G. (2021). A study about the role of the human factor in maritime cybersecurity. *SPOUDAI – Journal of Economics and Business*, 71 (1-2), 55-72. https://hdl.handle.net/10419/283673

[3] 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

[4] Canepa, M., Ballini, F., Dalaklis, D., Vakili, S. & Hernandez L., M., C. (2021). CR CyberMar as a solution path towards cybersecurity soundness in maritime logistics domain. *Transactions on Maritime Science*, 10 (1), 137-149. https://doi.org/10.7225/toms.v10.n01.011

[5] World Economic Forum (2025, January 13). Global cybersecurity outlook 2025. Retrieved from: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

[6] European Maritime Safety Agency (2021, October 1). Awareness in maritime cybersecurity. Retrieved from: https://www.emsa.europa.eu/we-do/safety/maritime-security/item/3477-cybersec.html

[7] Leloudas, G. (2021). Cyber risks, autonomous operations and risk perceptions. In: B. Soyer & A. Tettenborn (eds.), *Artificial intelligence and autonomous shipping: Developing the international legal framework* (pp. 101-118). Bloomsbury Publishing. https://doi.org/10.5040/9781509933389.ch-005

[8] Mensah, T. A. (2004). The place of the ISPS Code in the legal international regime. *WMU Journal of Maritime Affairs*, 3, 17-30. https://doi.org/10.1007/BF03195047

[9] Dalaklis, D. & Schröder-Hinrichs, J. U. (2019). The cyber-security element of hybrid warfare: Is there a need to "formalise" training requirements?. *Proceedings of the 10th NMIOTC Annual Conference, "Countering Hybrid Threats: An Emerging Maritime Security Challenge"*, Chania, Greece. https://doi.org/10.13140/RG.2.2.24684.82561

[10] Kitada, M., Baldauf, M., Mannov, A., Svendsen, P. A., Baumler, R., Schröder-Hinrichs, J.U., Dalaklis, D., Fonseca, T., Shi, X. & Lagdami, K. (2018). Command of vessels in the era of digitalization. In: Kantola, J. I., Nazir, S. & Barath, T. (eds.), *Advances in Human Factors, Business Management and Society* (pp. 339-350). Springer. https://doi.org/10.1007/978-3-319-94709-9_32

[11] Tonn, G., Kesan, J., Zhang, L. & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport Policy,* 79, 103-104. https://doi.org/10.1016/j.tranpol.2019.04.019

[12] Catteddu, D. & Hogben, G. (2009, November). Cloud Computing. Benefits, risks and recommendations for information security. European Union Agency for Cybersecurity. Retrieved from: https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Computing%20Security%20Risk%20Assessment.pdf

[13] Forbes (2017, August 16). NotPetya ransomware attack cost shipping giant Maersk over $200 million. Retrieved from: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#

[14] Soyer, B. & Tettenborn, A. (2021). *Artificial Intelligence and Autonomous Shipping: Developing the International Legal Framework*. Bloomsbury Publishing. https://www.bloomsbury.com/uk/artificial-intelligence-and-autonomous-shipping-9781509933358/ ; https://doi.org/10.5040/9781509933389

[15] International Maritime Organization (2022, June 7). Guidelines on maritime cyber risk management. Retrieved from: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

[16] Murphy, M., Hoffman, F. G. & Schaub, G. J. (2016). *Hybrid maritime warfare and the Baltic Sea Region*. Centre for Military Studies, University of Copenhagen. https://cms.polsci.ku.dk/publikationer/Hybrid_Maritime_Warfare_and_the_Baltic_Sea_Region.pdf

[17] European Commission, Directorate-General for Defence Industry and Space, Deloitte, KU Leuven, Doumbouya, L., De Man, P., León Vargas, C., Lacroix, L., Nikolov, M., Munters, W., Papadimitriou, A., Vancauwenberghe, G., Seghier, M., Vandenbroucke, D. & Wauters, P. (2022). *Pilot project on space traffic management – The rise of importance of space traffic management (STM): Final report.* Publications Office of the European Union. https://data.europa.eu/doi/10.2889/3462708

[18] de Andres Gonzalez, O., Koivisto, H., Mustonen, J. M. & Keinänen-Toivola, M. M. (2021). Digitalization in just-in-time approach as a sustainable solution for maritime logistics in the Baltic Sea Region. *Sustainability, 13* (3), 1173. https://doi.org/10.3390/su13031173

[19] Aro, E. & Rytter, N. G. M. (2020). *Maritime industry processes in the Baltic Sea Region. Synthesis of eco-inefficiencies and the potential of digital technologies for solving them*. ECOPRODIGI, Pan-European Institute, Turku School of Economics, University of Turku. https://ecoprodigi.eu/wp-content/uploads/2020/02/ECOPRODIGI-Research-Report-1-2020-final.pdf

[20] Shayan, J., Azarnik, A., Chuprat, S., Karamizadeh, S., Alizadeh, M. (2014). Identifying Benefits and Risks Associated with Utilizing Cloud Computing. https://doi.org/10.48550/arXiv.1401.5155

[21] Adonis (2024, February 13). The evolution of cloud-based solutions in maritime operations. Retrieved from: https://www.adonishr.com/blog/the-evolution-of-cloud-based-solutions-in-maritime-operations

[22] Digital Ship (2017, September 20). Maritime Cloud becomes Maritime Connectivity Platform. Retrieved from: https://thedigitalship.com/news/electronics-navigation/maritime-cloud-becomes-maritime-connectivity-platform/

[23] Riviera (2016, April 25). Maritime Cloud development holds promise for e-navigation. Retrieved from: https://www.rivieramm.com/opinion/opinion/maritime-cloud-development-holds-promise-for-e-navigation-33375

[24] European Union Agency for Cybersecurity (2023, January 31). *NIS Directive 2*. Retrieved from: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2

[25] Hafen Hamburg (2024, November 11). Finding digital port logistics services becomes simpler. Retrieved from: https://www.hafen-hamburg.de/en/press1/news/finding-digital-port-logistics-services-becomes-simpler/

[26] Ship & Offshore (2023, August 30). Gothenburg to revolutionise port call management. Retrieved from: https://www.shipandoffshore.net/news/ship-operation/detail/news/gothenburg-to-revolutionise-port-call-management.html

[27] Baltic Sea & Space Cluster (2021, February 7). Port of Gdańsk implements a new ERP system. Retrieved from: https://www.bssc.pl/2021/02/07/port-of-gdansk-implements-a-new-erp-system/

[28] International Association of Marine Aids to Navigation and Lighthouse Authorities. (2017, March). Maritime Cloud conceptual model. The Maritime Cloud Development Forum. Retrieved from: https://www.iala.int/content/uploads/2017/03/IALA-Input-paper-Maritime-Cloud-conceptual-model.pdf

[29] Nogal, M. & O'Connor, A. (2017). Cyber-transportation resilience: Context and methodological framework. In: Linkov, I. & Palma-Oliveira, J. (eds.), *Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security* (pp. 415-426). Springer. https://doi.org/10.1007/978-94-024-1123-2_15

[30] Hoeft, M., Gierlowski, K., Rak, J., Wozniak, J. & Nowicki, K. (2021). Non-satellite broadband maritime communications for e-navigation services. *IEEE Access,* 9, 62697-62718. https://doi.org/10.1109/ACCESS.2021.3074476

[31] European Commission (2025, May 17). A federated European FAIR and ppen Research ecosystem for oceans, seas, coastal and inland waters. Retrieved from: https://cordis.europa.eu/project/id/101094227

[32] European Commission (2022, October 28). Towards a green and sustainable ecosystem for the EU Port of the Future. Retrieved from: https://cordis.europa.eu/article/id/442407-creating-the-port-of-the-future

[33] Lange, H., Combes, B., Jermalavičius, T. & Lawrence, T. (2019). To the Seas Again. Maritime Defence and Deterrence in the Baltic Region. International Centre for Defence and Security. https://icds.ee/en/to-the-seas-again-maritime-defence-and-deterrence-in-the-baltic-region/; https://doi.org/10.4324/9780429289347-3

[34] Charamis, E., Charamis, D., Kyriakopoulos, G. L. & Ntanos, S. (2025). The Growth of Maritime Communications and Technology Related to the Trends in the Shipping Industry: A Financial Perspective. *Economies, 13* (4), 99. https://doi.org/10.3390/economies13040099

[35] European Maritime Safety Agency (2019, July 18). *Guidance and best practices.* Retrieved from: https://emsa.europa.eu/about/financial-regulations/download/5726/3611/23.html

[36] United Nations Conference on Trade and Development (2024, October 22). Review of maritime transport 2024. Retrieved from: https://unctad.org/publication/review-maritime-transport-2024

[37] Drougkas, A., Sarri, A., Kyranoudi, P. & Zisi, A. (2019). Port cybersecurity. Good practices for cybersecurity in the maritime sector. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/Good%20practices%20for%20the%20maritime%20security%20report.pdf

[38] European Parliament & Council of the European Union (2022, December 27). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. Retrieved from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[39] Agenzia per la Cybersicurezza Nazionale (2022, May 30). National cybersecurity strategy 2022-2026. Retrieved from: https://www.acn.gov.it/portale/en/strategia-nazionale-di-cybersicurezza

[40] Agence Nationale de la Sécurité des Systèmes d'Information (2024, February). Cyber threat overview 2023. Retrieved from: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-002.pdf

[41] Baltic and International Maritime Council (2024, November 14). Guidelines on cyber security on board ships (Version 5). Retrieved from: https://www.bimco.org/media/s4ddrsfe/2024-11-14-guidelines_on_cyber_security-v5-final.pdf

[42] Ivanov, D., Dolgui, A. & Sokolov, B. (2022). Cloud supply chain: Integrating Industry 4.0 and digital platforms in the "Supply Chain-as-a-Service". Transportation Research Part E: Logistics and Transportation Review, 160, 102676, https://doi.org/10.1016/j.tre.2022.102676

[43] Pinna, R., Veglianti, E., Musso, M. & De Marco, M. (2022). The impact of digital supply chain on operational a case study on cruise sector. In: E. Zaramenskikh & A. Fedorova (eds.), *Digitalization of Society, Economics and Management (Lecture Notes in Information Systems and Organisation,* vol 53, pp. 387-399). Springer. https://doi.org/10.1007/978-3-030-94252-6_29

[44] Tam, K., Moara-Nkwe, K. & Jones, K. (2021). A conceptual cyber-risk assessment of port infrastructure. University of Plymouth. https://pearl.plymouth.ac.uk/secam-research/1480

[45] Istituto per gli Studi di Politica Internazionale (2024, June 11). From maritime security to sea power: NATO's paradigm shift. Retrieved from: https://www.ispionline.it/en/publication/from-maritime-security-to-sea-power-natos-paradigm-shift-176619

[46] Ansa (2022, October 18). Cybersecurity:Porto Trieste scudo con tecnologia quantistica. Retrieved from: https://www.ansa.it/sito/notizie/economia/2022/10/18/cybersecurityporto-trieste-scudo-con-tecnologia-quantistica_44cb34f9-690b-481a-8680-b92e9f1191e0.html

[47] Ports of Genoa (2023, September 20). Sicurezza informatica, i Ports of Genoa al CSET 2023. Retrieved from: https://www.portsofgenoa.com/it/magazine/news/sicurezza-informatica-ports-of-genoa-cset-2023.html

[48] Ghorra, B. (2024, December 11). Strengthening France's Strategic Position in the Undersea Cable Sector. Retrieved from: https://incyber.org/en/article/renforcement-de-la-position-strategique-de-la-france-dans-le-domaine-des-cables-sous-marins/

[49] Francaix, J. (2018, October 15). SOGET et Microsoft: un partenariat stratégique pour une digitalisation sécurisée des ports français et mondiaux. Retrieved from: https://news.microsoft.com/fr-fr/2018/10/15/soget-et-microsoft-un-partenariat-strategique-pour-une-digitalisation-securisee-des-ports-francais-et-mondiaux/

[50] Fundación Valenciaport (2025, October 8). *Fundación Valenciaport will strengthen port cybersecurity with the European ATHENA project*. Retrieved from: https://www.fundacion.valenciaport.com/en/news-events/2025/10/fundacion-valenciaport-will-strengthen-port-cybersecurity-with-the-european-athena-project/

[51] Piraeus Smart Port (2023). Digital Transformation in Piraeus Port. Retrieved from: https://presentations.boussiasevents.gr/files/_boussias_conferences_content/presentations/shipit/2023/14b.Parthenis_ShipIT_23.pdf

[52] Center for International Maritime Security (2018, June 11). Countering hybrid threats in the maritime environment. Retrieved from: https://cimsec.org/countering-hybrid-threats-in-the-maritime-environment/

[53] Fincantieri (2025, July 8). Financial data 2025. Analyst and investor underwater day. Retrieved from: https://www.fincantieri.com/globalassets/investor-relations/presentazioni/eventi/2025/fincantieriuw_investorday.pdf

[54] Fincantieri (2025, June 26). Sustainability governance. Cyber security management. Retrieved from: https://www.fincantieri.com/en/sustainability/governance/cyber-security-management/

[55] Agenzia per la Cybersicurezza Nazionale (2025, July 3). Authority and sanctions. Retrieved from: https://www.acn.gov.it/portale/en/regolazione

[56] Microsoft (2025, February 28). What is Zero Trust?. Retrieved from: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview

[57] La Repubblica (2024, March 28). Dri (E-phors): "Abbiamo creato uno scudo high-tech per navi militari e da crociera". Retrieved from: https://www.repubblica.it/tecnologia/dossier/shiptech-robotica-digitale-e-green-il-futuro-a-bordo/2024/03/28/news/dri_e-phors_abbiamo_creato_uno_scudo_high-tech_per_navi_militari_e_da_crociera-422353325/

[58] International Society of Automation (2025, August 25). ISA/IEC 62443 series of standards. Retrieved from: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[59] Laurenza, G., Tacconi, R., Dri, M., Landucci, S. & Alì, D. (2025). Maritime Cyber Security Platform (MCSP). In: *Technology and Science for the Ships of the Future,* 10, 1154-1163. https://ebooks.iospress.nl/doi/10.3233/PMST250137

[60] Fincantieri (2025). Fincantieri and Accenture Announce the Launch of Fincantieri Ingenium. Retrieved from: https://www.fincantieri.com/en/media/press-releases/2025/fincantieri-and-accenture-announce-the-launch-of-fincantieri-ingenium/

[61] North Atlantic Treaty Organization (2024, May 7). Countering hybrid threats. Retrieved: from https://www.nato.int/cps/en/natohq/topics_156338.htm

[62] 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), 710. https://doi.org/10.3390/info15110710