CLOUD SERVICES AND MARITIME CYBERSECURITY IN THE BALTIC SEA REGION

Daisy Romanini
Institute of Informatics and Telematics, CNR
Pisa, 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 Advanced Studies School Lucca
Lucca, Italy
E-mail: fabio.pinelli@imtlucca.it

Marinella Petrocchi
Institute of Informatics and Telematics, CNR
Pisa, Italy
E-mail: marinella.petrocchi@iit.cnr.it

UDK 004.77:656.61(262.24)

Abstract

The maritime sector in the Baltic Sea region is undergoing rapid digital transformation, with growing adoption of cloud-based technologies in fleet management, logistics, and port operations. While these innovations offer improved efficiency and coordination, they also expose critical systems to evolving cybersecurity risks. This paper explores the intersection of maritime digitalization and cybersecurity in the Baltic context, with a particular focus on the adoption of cloud services. Drawing on a qualitative, interpretative approach (referencing legal frameworks, illustrative case studies, stakeholder concerns, and regional policy documents), the study identifies key vulnerabilities, including reliance on third-party cloud providers, fragmented regulatory implementation, and gaps in cross-border coordination. Given the Baltic Sea's strategic significance in European and global trade, the analysis highlights the need for harmonized cybersecurity frameworks, structured threat intelligence sharing, and investment in maritime-specific training and secure digital infrastructure. By framing current challenges in light of legal, operational, and geopolitical dynamics, the paper contributes to a broader understanding of how regional cooperation can enhance maritime cybersecurity resilience in an increasingly contested digital environment.

Keywords: Maritime Cybersecurity, Cloud Computing, Baltic Sea Region, Digital Resilience, Critical Infrastructure Protection

1. LEGAL AND REGULATORY FRAMEWORKS

Ex facto oritur ius is a Latin aphorism and legal principle that refers to the development of law after certain events occur. A clear illustration of this is the attacks of 9/11, which alerted the International Maritime Organization (IMO) to the importance of managing security risks in the maritime domain and led to the implementation of the International Ship and Port Facility Security ISPS Code [15, 17].

Today, the maritime industry is experiencing a significant digital transformation, characterized by a growing dependence on technologies. This change is driven by the need for improved efficiency, reduced operating costs, and greater data accessibility. However, this transition is not exempt from inconveniences; the adoption of innovative technologies introduces diverse cybersecurity challenges that pose threats to the safety of maritime activities.

The ongoing discussions on the digitalization phenomenon and Maritime Autonomous Surface Ships (MASS) illustrate how the shipping industry may undergo significant change in the near future [3, 12]. Considering this, as well as the increasing utilisation of Information Technologies (IT) applications by a large number of shipping companies, addressing cybersecurity issues effectively within the maritime domain through proper mitigation measures ought to be a high-priority concern.

Following the ideas presented by Tonn [23], transport systems have four layers of cyber systems: The first is the perceptual layer, which uses elements such as GPS and wireless sensors to connect physical and cyber systems. The second layer is the network systems that transfer information, such as satellite networks or the internet. The third layer includes cloud services and intelligent computing that support systems, and the fourth layer is the one that relates to applications that connect the physical world with cyber systems.

Modern ships are equipped with integrated navigation and communication systems that encompass all four previously mentioned layers. This integration allows perpetrators to disrupt maritime operations remotely, without exposing themselves to physical security measures, unlike the attacks of 9/11 [23]. As a result, the potential risk of harm to life and damage to property at sea is significantly increased.

The concept of cloud services, identified within the third aforementioned layer, originates from the premise of offering consumers hardware resources, middleware platforms, and software as services. The main current service models are: *Software as a Service* (SaaS), *Platform as a Service* (PaaS) and *Infrastructure as a Service* (IaaS). Such models can be utilised in different stages of shipping operations, for instance, many shipping companies use SaaS Platforms to provide their customers access to real-time data on shipment status; Shipping companies may also rely on IaaS to store data securely and provide information recovery options by ensuring data is properly backed up. Nowadays, the reliance on these services is increasing as the industry moves forward to digitalization and automation of processes [19].

As mentioned before, the application of these technologies is most commonly viewed to enhance operational efficiency, and to reduce costs. However, the industry has already learnt from some of the weak points that their use may bring. Most probably, a very well-known example in this category took place in 2017; when the IT systems of the then world´s second largest shipping company Maersk Shipping Line[1] were literally brought to a complete halt by the Maersk NotPetya malware, resulting in business interruption and losses amounting to $200 - $300 million USD[2]. This incident was not a stand-alone case; another big disruption happened in the Black Sea, where at least 20 vessels appeared in the Automatic Identification System (AIS) 20 miles inland, very close to a Russian airport, misdirecting the signal and leaving the operators in a state of false security [22]. The IMO was alerted by these incidents, and certain pressures from the wider industry following which through its Maritime Safety Committee (MSC) adopted Resolution MSC.428(98) requiring cybersecurity risks to be managed as part of the ship´s Safety Management System (SMS), marking it mandatory for shipowners to treat cybersecurity as a key component of maritime safety; marking a significant step ahead in addressing cybersecurity in the maritime sector.

Additionally, in 2022, after having realised the urge to raise awareness on cyber risk threats, IMO´s MSC together with its Facilitation Committee (FAL) adopted the Guidelines on maritime cyber risk management. Although the guidelines are not mandatory for member States, they provide high-level recommendations on maritime cyber risk management to prevent shipping from emerging cyber threats and

[1] According to Marine Insight, in a report by Zahra Ahmed. Retrieved from: https://www.marineinsight.com/know-more/best-shipping-companies-in-merchant-navy/. All urls have been accessed on May 20, 2025.
[2] According to a statement issued by A. P. Møller -Mærsk A/S. Retrieved from: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#

vulnerabilities, encouraging safety and security management practices in the cyber domain (MSC-FAL.1/Circ.3/Rev.2) [11].

Furthermore, in Europe, the regulatory framework addressing cyber security specifically dealing with cloud services, is the NIS2 Directive[3] (Network and Information Security Directive 2), which is in force since 2022, and replaces the original NIS Directive. It has a broader scope covering maritime operators as it is designed to combat emerging cyber-security threats and improve the resilience of key stakeholders in the maritime industry, such as ports, shipping companies, and service providers [18].

This specific Directive mandates that entities applying cloud services for shipping operations must implement risk management measures, to identify vulnerabilities and prevent cyber risks. One of the key components of this Directive is the incident reporting, which allows stakeholders to be aware of important cyber threats occurring within the domain. Under this Directive, *incident* means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems[4]. Introducing a communication system capable of alerting entities and authorities of any of such incidents.

Cutting a long way short, cloud services and technologies play a vital role in the shipping industry by facilitating processes, improving operational efficiency, and reducing costs. However, it is important to bear in mind the security implications that the application of these services brings [16], and the approach that Organizations shall take to effectively prevent such risks and reduce them.

Research Aim. This paper aims to analyse how the integration of cloud services is reshaping cybersecurity practices within the maritime sector, with a specific focus on the Baltic Sea region. As cloud technologies become more embedded in operational processes, the study identifies associated risks (from data breaches to service disruptions) and explores how coordinated regulatory and institutional responses can improve regional resilience.

Although there is much more to be done, the collaboration among shipping organizations, regulatory bodies, and computer security experts is essential in safeguarding the integrity and security of shipping operations in a rapid and increasingly digital and technological world.

2. METHODOLOGY

This study employs a qualitative, interpretative methodology to examine how cloud integration is reshaping cybersecurity dynamics in the Baltic Sea's maritime sector. Drawing on legal analysis, technical evaluation, and comparative policy review, the research explores both structural vulnerabilities and institutional responses to emerging cyber risks. This approach reflects the increasingly interconnected nature of maritime infrastructure, where cloud services, regulatory frameworks, and threat landscapes converge across national borders.

To ensure depth and cross-validation, the study triangulates insights from four key source categories:

- Legal and regulatory frameworks, including the NIS2 Directive, the ISPS Code, and IMO cybersecurity guidance (e.g., MSC-FAL.1/Circ.3/Rev.2), are referenced to illustrate current norms and regulatory efforts in maritime cybersecurity;
- Operational case studies, such as the 2017 NotPetya attack on Maersk and GPS spoofing incidents in the Black Sea, are cited as examples highlighting relevant vulnerabilities in maritime digital systems;
- Institutional and policy reports from EU agencies (e.g., ENISA, the European Commission), national cybersecurity bodies, and sectoral initiatives (e.g., Blue-Cloud 2026, EMODnet) are mentioned to contextualize cloud adoption trends, preparedness levels, and coordination gaps;

[3] DIRECTIVE (EU) 2022/2555 of the European Parliament and of the Council of 14 Dec. 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation EU No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). In force since December 14, 2022.
[4] DIRECTIVE (EU) 2022/2555 Article 6 (6).

- Academic and technical literature on maritime digitalization, cyber-physical risks, and regional cooperation is drawn upon to support the framing of key themes in the research.

A purposive sampling approach was used to select incidents and policy initiatives that demonstrate critical fault lines in the regional cybersecurity ecosystem; especially those revealing tensions between technological innovation, strategic vulnerability, and regulatory lag. Emphasis was placed on cases and programs with implications for digital sovereignty, hybrid threat resilience, and cross-sector interoperability.

3. E-NAVIGATION AND CLOUD IN THE BALTIC REGION

As maritime operations become increasingly digitized, regulatory compliance remains central to maintaining safety and legal integrity at sea. Frameworks such as the International Safety Management (ISM) Code, the Maritime Labour Convention (MLC), and evolving IMO environmental regulations form the backbone of global maritime governance. In 2025, cloud-based compliance tools have become critical enablers of these frameworks. These platforms offer real-time access to regulatory updates, digital audit trails, and automated compliance checklists, helping companies meet obligations efficiently and minimize the risks of fines, delays, and reputational harm [13].

The broader maritime digital transformation has been significantly advanced by cloud technology, most notably through the development of the Maritime Connectivity Platform (MCP), formerly known as the Maritime Cloud. Initiated under the EU-funded EfficienSea2 project and led by the Danish Maritime Authority (DMA), MCP provides a secure, service-oriented infrastructure for exchanging operational and navigational data. Its core components include a Service Registry for accessing digital tools such as route optimization and weather integration, and an Identity Registry to authenticate users across national and institutional boundaries [5].

First introduced at the 2016 International e-Navigation Underway Conference, the Maritime Cloud (now MCP) was envisioned as a unified communication framework to enhance navigational safety, security, and efficiency. DMA's Director of Technology, Omar Frits Eriksson, highlighted its potential to bridge fragmented systems and enable reliable data interoperability. Over time, the platform has evolved by incorporating lessons from international initiatives such as Sweden's STM Validation Project and South Korea's SMART Navigation Project [21].

By 2025, MCP has transitioned from concept to implementation, supporting data integrity, confidentiality, and authenticity for a wide range of maritime stakeholders. Its design aligns with the EU's NIS2 Directive, which mandates cyber-risk management, regular audits, and incident reporting for critical infrastructure operators, including those in maritime logistics [6].

This shift is especially visible in the Baltic region, which has emerged as a European leader in maritime digitalization. Ports such as Hamburg[5], Gothenburg[6], and Gdańsk[7] have adopted cloud-based Port Community Systems using SaaS models to enhance communication among customs, terminals, agents, and logistics providers. These systems reduce administrative burdens and improve vessel turnaround efficiency [10].

[5] Port customers have access to the "Marketplace.Hamburg" platform, which provides a centralized interface for a range of digital port logistics services. These include tools such as online port fee declarations, waiting berth information for inland vessels, the eDeclaration ship registration portal, and slot booking via Truckgate. The platform brings together services offered by key partners, including HPA, DAKOSY, and HVCC. Retrieved from: https://www.hafen-hamburg.de/en/press/news/finding-digital-port-logistics-services-becomes-simpler/?utm_source=chatgpt.com

[6] In early 2024, the Port of Gothenburg introduced Digital Port Call, a software system developed in collaboration with Finnish port operations specialist Awake.AI. The platform consolidates essential information related to port calls and provides all stakeholders with improved transparency. Its deployment has contributed to greater efficiency, reduced waiting times, and lower emissions. Retrieved from: https://www.shipandoffshore.net/news/ship-operation/detail/news/gothenburg-to-revolutionise-port-call-management.html?utm_source=chatgpt.com

[7] The Port of Gdańsk has implemented the Comarch ERP XL system, developed by Poland's largest software manufacturer. This enterprise resource planning system integrates accounting, controlling, and HR functions, facilitating enterprise management and the flow of documents and key information. While not a traditional PCS, this system enhances operational efficiency and supports the port's digital transformation efforts. Retrieved from: https://www.bssc.pl/2021/02/07/port-of-gdansk-implements-a-new-erp-system/?utm_source=chatgpt.com

To illustrate how cloud technologies underpin contemporary maritime operations, Table 1 presents the three primary cloud service models (SaaS, PaaS, and IaaS) along with their specific roles in port operations, logistics, and vessel services.

Table 1 Cloud Models in Maritime Sector

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: International Organization for Marine Aids to Navigation

Despite progress, digital maturity varies significantly across the region. While ports in Germany, Denmark, and Sweden boast advanced infrastructures, others (such as those in Estonia or Latvia) face budgetary and technical limitations. This unevenness poses cybersecurity risks and complicates cross-border coordination. ENISA has flagged the absence of a unified cyber-risk assessment methodology across EU ports as a major challenge to securing the digital maritime ecosystem [6].

At the international level, former IMO Secretary-General Kitack Lim stressed the need for harmonised data and interface standards to support seamless maritime communication. He also suggested the IMO could eventually take on greater responsibility for digital maritime infrastructure. DMA Director General Andreas Nordseth has underscored that the full potential of maritime digitalisation will only be realised if backed by responsive and market-driven governance structures [20].

4. THREATS TO MARITIME CYBERSECURITY

The availability of high-speed broadband on land has enabled a rapid proliferation of advanced digital services through terrestrial networks. However, this progress has not been mirrored offshore due to the limitations of digital communication technologies in maritime environments. Despite the ambitions outlined in the e-navigation initiative, which defines a set of Maritime Services, evolution in maritime ICT systems has been relatively slow. Only a handful of systems, such as the VHF Data Exchange System (VDES) and the TRI-Media Telematic Oceanographic Network (TRITON), have emerged to extend traditional radio-communication services, yet even these face significant technical and operational limitations [9].

At the same time, the accelerating shift toward cloud-based maritime operations is fundamentally reshaping the cybersecurity landscape in the Baltic Sea region. While cloud technologies enhance efficiency, real-time data access, and interconnectivity among maritime stakeholders, they also introduce a wide array of cyber vulnerabilities. These risks grow in scope and complexity as ports, vessels, logistics providers, and governmental authorities become part of a tightly interlinked digital ecosystem.

Survey data from EMODnet partners reveal widespread concern about these developments. Respondents expressed apprehension regarding data confidentiality, licensing restrictions, third-party mismanagement, and the legal ambiguities surrounding jurisdiction (especially with U.S.-based cloud providers). Particular anxiety centered on sensitive data types, such as proprietary research datasets and biological data under moratorium or licensing conditions. A respondent noted, for instance, "*The data is like currency for research institutions. If abused or used without credit, it's like taking credentials for the research work*" [10].

To address such concerns, the Blue-Cloud 2026 initiative is working to extend the pilot Blue-Cloud infrastructure into a federated, secure European data ecosystem. Grounded in FAIR data principles and aligned

with the European Open Science Cloud (EOSC), the project facilitates secure, cross-border access to aquatic data for scientific, regulatory, and commercial applications. By integrating marine data sources such as EMODnet, Copernicus, and SeaDataNet with European e-infrastructures like EUDAT, D4Science, and WEkEO, the initiative supports strategic goals including the EU Green Deal, the Digital Twin of the Ocean, and the UN Sustainable Development Goals [8].

As introduced earlier, a helpful way to conceptualize technical vulnerabilities in maritime cloud ecosystems is through the four-layer cyber-physical model proposed by Tonn. This model consists of:

1. Perceptual Layer: Includes physical inputs such as GPS, AIS, sensors, and radars. These are susceptible to spoofing and jamming attacks, which distort navigational data.
2. Network Layer: Facilitates data transmission through satellite and terrestrial communication links. This layer is vulnerable to denial-of-service (DoS), man-in-the-middle attacks, and packet sniffing.
3. Cloud and Computing Layer: Where data is stored, processed, and analyzed. Misconfigurations, insider threats, and zero-day exploits pose major risks here, particularly with third-party vendors outside the EU legal framework.
4. Application Layer: The user interface, including dashboards, port management tools, and navigation software. Common threats include phishing, credential stuffing, and malware delivery through insecure access points [23].

To better illustrate the complex and multifaceted nature of cyber threats targeting maritime cloud systems, Figure 1 presents a visual representation of the cyber-attack surface within these ecosystems. This diagram highlights key threat vectors (including malware, phishing, network attacks, and unauthorized access) and their potential impact on critical components such as vessel systems, port systems, logistics platforms, and sensitive data repositories. By conceptualizing how these vulnerabilities impact different cloud service models (SaaS, PaaS, IaaS), the figure highlights the interconnected nature of maritime digital systems and emphasizes the importance of robust cybersecurity measures.

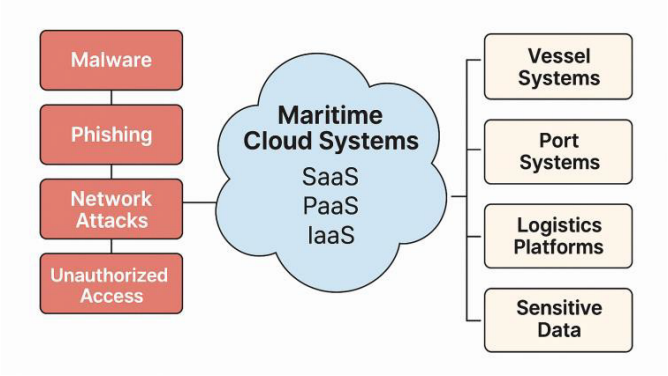

Figure 1 Cyber-Attack Surface in Maritime Cloud Systems

Source: Own elaboration

Historical incidents highlight the severity of these vulnerabilities. The 2017 NotPetya ransomware attack severely disrupted Maersk's global operations, including terminals in Gdańsk and Gothenburg, causing losses that exceeded $250 million. Similarly, GPS spoofing near the Black Sea has raised alarms about the potential for replication in high-traffic Baltic waters [22, 23].

Cybersecurity risks are further exacerbated by legacy infrastructure. Many ports continue to operate on outdated SCADA systems that lack modern security features, leaving integration points exposed when interfaced with newer cloud platforms [6]. Human factors also remain a persistent concern. EMODnet survey responses revealed that many maritime personnel have limited cybersecurity training, with poor password practices, inadequate authentication measures, and the increased use of personal devices, all of which have intensified since the COVID-19 pandemic [11].

Service agreements with cloud providers often add another layer of complexity. Many stakeholders operate under vague Service Level Agreements (SLAs) that offer limited clarity on accountability, breach notification procedures, or legal jurisdiction, especially when involving providers based outside the EU [7].

5. REGIONAL COORDINATION AND POLICY GAPS

While technical vulnerabilities pose immediate risks to maritime operations, they also expose deeper issues related to governance and institutional readiness. Addressing these challenges requires a closer examination of how regional policies, coordination mechanisms, and legal frameworks influence the Baltic Sea region's ability to respond to evolving cyber threats.

The Baltic region faces a fragmented cybersecurity landscape shaped by varying levels of digital maturity and political commitment among littoral states. The NIS2 Directive has established a foundational EU-wide cybersecurity framework, yet its implementation remains inconsistent. While countries like Sweden and Germany have developed advanced maritime cybersecurity protocols and dedicated response units, others continue to lack updated threat response plans or adequate institutional support, resulting in policy blind spots across the region [7]. These disparities are particularly problematic in cloud-based environments, where cyber threats easily cross national boundaries.

A central challenge is the absence of a unified, region-specific system for real-time cyber threat intelligence sharing tailored to the maritime sector. While national CERTs (Computer Emergency Response Teams) exist, they generally operate independently. Cross-border cooperation tends to rely on informal arrangements or voluntary agreements, rather than binding structures. Furthermore, the lack of standardized data-sharing formats and protocols hinders timely and coordinated responses, limiting situational awareness across stakeholders [6]. Although frameworks like the IMO's MSC-FAL.1/Circ.3/Rev.2 provide useful guidelines, their voluntary nature results in uneven uptake, weakening efforts toward broader standardization [11].

Recent text mining research on 155 academic studies related to maritime sustainability reveals an underdeveloped focus on digitalization. While port sustainability, emissions reduction, environmental regulations, and cost optimization are well-represented, topics like cybersecurity, digital integration, and coordinated information sharing remain significantly overlooked [4].

Nevertheless, pilot initiatives such as the Sea Traffic Management (STM) system in the Ports of Rauma and Gävle illustrate the operational benefits of improved digital coordination. 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 [4]. 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 [1].

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 [1, 14].

The Baltic Sea's economic and strategic significance further underscores the urgency of coordinated action. With over 881 million tonnes 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 [14]. 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 [2].

Finally, unresolved legal and financial risks continue to undermine trust in cloud-based maritime systems. Insurance policies often lack clear definitions regarding coverage for cloud-related cyber incidents, especially those involving third-party providers. Legal ambiguity around liability and breach response mechanisms makes it difficult to ensure accountability or secure compensation after an incident. Without enforceable legal frameworks, stakeholders may remain hesitant to fully adopt cloud services in high-risk operational settings [22].

6. RECOMMENDATIONS AND CONCLUSION

To address the growing cybersecurity threats facing cloud-integrated maritime systems in the Baltic Sea region, a coordinated, multi-tiered response is urgently needed. Given the region's geopolitical sensitivities, economic significance, and accelerating digital transformation, an effective strategy must combine regulatory alignment, technical safeguards, industry-driven incentives, and enhanced regional threat intelligence coordination.

One proposed measure is the establishment of a permanent multilateral institution dedicated to maritime cybersecurity governance in the Baltic. This body would facilitate the consistent implementation of the NIS2 Directive across Baltic Sea states, promote interoperability among national cybersecurity frameworks, coordinate cross-border incident response exercises, and oversee a secure, shared threat intelligence platform. Such an institution could close existing gaps in CERT cooperation and foster a more unified and responsive regional cyber defense posture.

A sector-specific certification scheme for maritime cloud services could further strengthen security baselines. This framework should be aligned with ENISA recommendations and IMO guidelines (e.g., MSC-FAL.1/Circ.3/Rev.2), and include independent third-party audits of cloud service providers supporting critical maritime infrastructure. This would enhance transparency, standardize practices, and increase trust in cloud-based systems.

Regional actors such as the European Maritime Safety Agency (EMSA) should take the lead in developing and implementing standardized training and certification programs focused on maritime cybersecurity. These programs should combine technical skills (such as secure cloud architecture design, encryption methods, and network segmentation) with policy education on legal compliance, risk management, and contract negotiation with service providers. Accredited, region-wide training would help bridge current workforce skill gaps and support consistent operational resilience.

To encourage private sector investment in secure digital infrastructure, governments should introduce financial incentives such as subsidies, tax credits, or grants tied to the use of certified cloud services. In parallel, public-private partnerships between technology firms and maritime stakeholders should be expanded to accelerate the adoption of innovative, secure digital solutions. Lessons from pilot projects like Sea Traffic Management (STM) implementations in Rauma and Gävle provide valuable models for such collaborations [4]. Additionally, the development of a Baltic Sea Hybrid Threats Fusion Cell has been proposed, modeled on the EU INTCEN Hybrid Fusion Cell. This center would provide strategic intelligence on hybrid and cyber threats, facilitate coordination with NATO, and strengthen the region’s early warning and analytical capacities. Such a node could play a pivotal role in countering hostile cyber operations and reinforcing resilience across the maritime domain [17].

The rapid uptake of cloud-based services in Baltic maritime logistics reflects a broader shift in global transport and supply chain management. While this transformation offers significant benefits (including operational efficiency, sustainability, and real-time coordination), it also expands the attack surface for cyber threats. Without harmonized regulations, technical standards, and shared intelligence systems, critical infrastructure remains exposed to disruptions by cybercriminals, system failures, or state-sponsored attacks.

Although this study focuses on the Baltic Sea region, comparing its cybersecurity posture with other key maritime zones can provide valuable context. Regions such as the North Sea, the Mediterranean, and the South China Sea face distinct geopolitical pressures, regulatory environments, and technological adoption levels. For example, the North Sea benefits from relatively mature cybersecurity cooperation mechanisms due to strong EU integration, whereas the Mediterranean exhibits greater variability in digital infrastructure and coordination. Drawing insights from such regions could help Baltic stakeholders identify adaptable strategies and avoid common pitfalls.

That said, several limitations of this study must be acknowledged. The regional focus, while providing depth, limits the generalizability of findings beyond the Baltic context. Furthermore, access to reliable data on maritime cyber incidents remains constrained due to national security sensitivities and commercial confidentiality. Disparities in digital maturity among Baltic nations also affect uniform implementation of best practices. Finally, the fast-evolving nature of both cloud technologies and cyber threats means that today's recommendations may require adaptation in the near future.

Future research should build on this work by conducting comparative analyses across global maritime regions, examining how different governance models, threat landscapes, and public-private dynamics shape cybersecurity outcomes. In addition, exploring the role of international memoranda of understanding (MOUs) under IMO frameworks may offer insights into strengthening interregional cooperation and harmonization of maritime cyber standards.

In conclusion, securing the future of the Baltic Sea's maritime sector in a digital age will depend on collective, forward-looking action. Regional coordination must include standardized legal and technical frameworks, synchronized policy implementation, targeted investment in workforce training and resilient infrastructure, and deepened public-private cooperation. Only through such comprehensive and collaborative efforts can the Baltic remain a secure, efficient, and strategically vital corridor for global maritime trade.

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

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 EU [grant agreement No. 101120688].

Conflict 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 paper.

Acknowledgements: The authors thank Professor Michael Ekow Manuel of the World Maritime University, Sweden, for fostering the initial connection that led to this collaboration.

REFERENCES

[1] 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, Finland. https://www.utupub.fi/bitstream/handle/10024/156199/ECOPRODIGI%20Research%20Report%201%202020%20 final.pdf?sequence=1

[2] 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

[3] 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, 4 June 2019. https://doi.org/10.13140/RG.2.2.24684.82561

[4] 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

[5] Digital Ship. (2017). *Maritime Cloud becomes Maritime Connectivity Platform*. https://thedigitalship.com/news/electronics-navigation/maritime-cloud-becomes-maritime-connectivity-platform/

[6] ENISA. (2023). *NIS Directive 2*. https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2

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

[8] European Commission. (2023). *A federated European FAIR and Open Research Ecosystem for oceans, seas, coastal and inland waters*. https://cordis.europa.eu/project/id/101094227

[9] Hoeft, M., Gierlowski, K., Rak, J., Wozniak, J., Nowicki, K. (2021). *Non-Satellite Broadband Maritime Communications for e-Navigation Services*. IEEE Access, Vol. 9, pp. 62697–62718. https://doi.org/10.1109/ACCESS.2021.3074476

[10] IALA. (2017). *Maritime Cloud conceptual model*. The Maritime Cloud Development Forum, International Organization for Marine Aids to Navigation. https://www.iala.int/content/uploads/2017/03/IALA-Input-paper-

[11] Maritime-Cloud-conceptual-model.pdf

[12] IMO. (2022). *Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2)*. International Maritime Organization. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

[13] Kitada, M. et al. (2018). *Command of Vessels in the Era of Digitalization*. In: Advances in Human Factors,

[14] Business Management and Society, pp. 339–350. http://dx.doi.org/10.1007/978-3-319-94709-9_32

[15] Kviteberg, B. (2024). *The Evolution of Cloud-Based Solutions in Maritime Operations*. https://www.adonishr.com/blog/the-evolution-of-cloud-based-solutions-in-maritime-operations

[16] 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, Estonia. https://icds.ee/en/to-the-seas-again-maritime-defence-and-deterrence-in-the-baltic-region/

[17] Leloudas, G. (2021) *Cyber Risks, Autonomous Operations and Risk Perceptions. Is a new liability paradigm required?.Artificial Intelligence and autonomous shipping*. In: Soyer, B., Tettenborn, A., Developing the international legal framework, pp. 101-117. ISBN 9781509933365. https://doi.org/10.5040/9781509933389.ch-005

[18] Matthews, T. (2019). *A brief history of cybersecurity*. https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/

[19] Mensah, T. (2003). *The place of the ISPS Code in the Legal International Regime. For the Security of International Shipping*. WMU Journal of Maritime Affairs, Vol. 3, pp. 17.

[20] Murphy, M., Hoffman, F. G., Schaub, G. J. (2016). *Hybrid Maritime Warfare and the Baltic Sea Region*. Centre for MilitaryStudies, University of Copenhagen. https://cms.polsci.ku.dk/publikationer/Hybrid_Maritime_Warfare_and_the_Baltic_Sea_Region.pdf

[21] NIST - National Institute of Standards and Technology. (2011). *Special Publication 800-145: The NIST Definition of Cloud Computing*. US Department of Commerce. https://csrc.nist.gov/pubs/sp/800/145/final

[22] 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. Springer, Dordrecht. https://doi.org/10.1007/978-94-024-1123-2_15

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

[24] Soyer, B., Tettenborn, A. (2021). *Artificial Intelligence and Autonomous Shipping: Developing the International Legal Framework*. Bloomsbury Academy. ISBN: 1509933352, 9781509933358.

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