ISSN: 2473-4901
v12 n6744

Governance as Attack Surface: Regulatory Fragmentation and Gray-Zone Cyber Threats in the Maritime Transportation System

Bilge Karabacak
karabacakb@uncw.edu

Ulku Yaylacicegi Clark
karabacakb@uncw.edu

Hosam Alamleh
alamlehh@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28403

Abstract

The Maritime Transportation System (MTS) relies on converged digital and physical infrastructure across vessels, ports, and logistics networks, and the ongoing integration of information technology with operational technology has substantially widened the maritime cyberattack surface. Although several international and national regulatory frameworks address maritime cyber risk, their fragmented scope, uneven enforcement, and inconsistent implementation may create gaps that sophisticated adversaries can exploit. Using a secondary qualitative synthesis of findings reported in the published MTS Cybersecurity Technology Roadmap, this study examines how regulatory fragmentation may increase the sector's exposure to gray-zone maritime cybersecurity threats. The analysis identifies four weaknesses: fragmented governance, inadequate workforce readiness, limited IT/OT asset visibility, and underdeveloped incident response and recovery, each of which may contribute to delays in detection, attribution, and recovery when incidents occur. Based on these findings, the study proposes the Vulnerability Cycle for Gray-Zone Activities, a conceptual model showing how governance gaps may function as cybersecurity attack surfaces that can be exploited through regulatory ambiguity and operational interdependence to generate disruption while remaining below the threshold of conventional armed conflict. The findings support regulatory harmonization, clearer governance and enforcement, stronger workforce readiness, and improved technical visibility and response capability.

Keywords: maritime cybersecurity, regulatory fragmentation, gray-zone operations, IT/OT convergence, maritime governance, cyber resilience

Governance as Attack Surface: Regulatory Fragmentation and Gray-Zone Cyber Threats in the Maritime Transportation System

Bilge Karabacak, Ulku Yaylacicegi Clark and Hosam Alamleh

1. INTRODUCTION

The Maritime Transportation System (MTS) depends on networked shipboard systems, port management platforms, and interconnected supply chain services. While these systems improve operational efficiency, they also expand the cyberattack surface (Afenyo & Caesar, 2023; Akpan et al., 2022). Due to the integrated systems, cybersecurity in MTS is not limited to information technology (IT) security anymore. It now impacts operational technology (OT), physical safety, port continuity, and national economic security (Afenyo & Caesar, 2023; Akpan et al., 2022).

More than 80% of the volume of international trade in goods is carried by sea. This makes maritime cybersecurity essential to global supply chains (United Nations Trade and Development [UNCTAD], 2024). Disruptions to major maritime routes and chokepoints can extend shipping routes, increase costs, and affect food and energy supplies, illustrating the broader consequences that cyber-enabled maritime disruption could also produce (UNCTAD, 2024). As maritime operations become more digitized, cyberattacks against MTS systems can create consequences for global trade in addition to the individual organizations.

Existing maritime cybersecurity research has extensively examined technical vulnerabilities (Afenyo & Caesar, 2023; Akpan et al., 2022; Martin & Benson, 2023), while unresolved questions remain regarding how fragmented governance and regulatory authority shape sector-wide cyber resilience. This study addresses this gap by examining how regulatory fragmentation may create conditions favorable to gray-zone cyber operations in the maritime domain.

Maritime cybersecurity regulation remains fragmented. Different organizations may be subject to different standards, authorities, inspection practices, and reporting expectations. This fragmentation can create uncertainty about who is responsible for identifying cyber risk, enforcing controls, sharing incident information, coordinating response, and supporting recovery. The problem becomes more serious because maritime operations are highly interdependent. Disruption affecting a vessel, a port, or logistics provider can quickly affect wider supply chain activity.

Regulatory fragmentation may create structural conditions favorable to gray-zone cybersecurity threats in the maritime domain. Gray-zone operations are designed to create strategic disruption without crossing the threshold of conventional military conflict. Maritime cyber incidents of this kind typically manifest as technical malfunctions, communications outages, navigation irregularities, or port-system failures that are difficult to distinguish from routine operational problems. When regulatory authority is unclear and response processes are inconsistent, malicious activity may therefore remain undetected or unresolved for longer periods.

The study addresses three questions: (1) How does regulatory fragmentation create cybersecurity gaps across MTS stakeholders? (2) Through what mechanisms do these gaps amplify exposure to gray-zone cyber threats? (3) What governance and technical measures could reduce this exposure? These questions are addressed through qualitative synthesis of expert-derived findings from the MTS Cybersecurity Technology Road Mapping (TRM) process, organized around the NIST Cybersecurity Framework 2.0.

This paper synthesizes maritime cybersecurity literature, regulatory guidance, and expert-derived TRM findings to develop the Vulnerability Cycle for Gray-Zone Activities and examine how governance fragmentation may create conditions favorable to gray-zone cyber activity.

2. LITERATURE REVIEW AND BACKGROUND

The literature examined in this study centers on the maritime cyber-threat landscape, risks from IT/OT convergence, current regulatory frameworks and their gaps, and gray-zone threat theory in the maritime domain.

The review draws on peer-reviewed research for scholarly evidence and regulatory, government, and industry sources for current standards, implementation requirements, and operational context.

2.1 Gray-Zone Threats in the Maritime Domain

The concept of gray-zone conflict refers to coercive activities that occur in the space between routine geopolitical competition and open armed conflict. It is deliberately calibrated to remain below thresholds that would trigger a conventional military response (Mazarr, 2015). Cyber operations have become an important instrument within this space because they provide opportunities for disruption, coercion, signaling, and intelligence collection without necessarily provoking immediate escalation (Ferazza & Mersinas, 2025). In the maritime domain, gray-zone activities have historically included territorial encroachment, fisheries interference, and interference with freedom of navigation. The cyber dimension of such operations is increasingly recognized as a threat vector. Letts (2024) argues the maritime domain is structurally susceptible to this threat vector given its legal ambiguity and multinational governance arrangements.

Unlike cybercrime, routine espionage, sabotage, or technical failure, gray-zone cyber activity involves strategic disruption or coercion deliberately calibrated below the threshold of armed conflict while exploiting ambiguity or plausible deniability.

Gray-zone cyber activity may exploit the complexity and interdependence of the MTS, where the involvement of actors across multiple jurisdictions means that even relatively minor cyber disruptions can produce disproportionate operational effects. The operational significance of this approach comes from its ambiguity, as maritime cyber incidents are frequently indistinguishable from technical malfunctions, human error, or equipment failure, providing the plausible deniability that gray-zone doctrine prizes. Drawing on gray-zone theory and maritime cybersecurity literature (Mazarr, 2015; Letts, 2024; Ferazza & Mersinas, 2025), Table 1 synthesizes characteristics relevant to maritime gray-zone cyber activity.

Characteristic	Distinguishing feature	Maritime example
Attribution ambiguity	Difficult to determine intent or responsible actor	AIS spoofing or GNSS manipulation
Limited escalation	Disruption without overt physical destruction	Temporary port-system or logistics disruptions
Economic coercion	Creates operational or commercial pressure	Cargo delays or supply-chain disruptions
Strategic uncertainty	Introduces confusion into operational decision-making	Navigation or communications interference

Table 1. Summary of distinguishing characteristics of maritime gray-zone cyber activity

From a cybersecurity perspective, these characteristics involve ambiguous attribution, limited escalation, and strategic disruption; in the maritime context, multinational governance, interconnected IT/OT systems, and cross-jurisdictional operations can further complicate detection, attribution, and coordinated response.

The literature connecting gray-zone theory directly to maritime cybersecurity remains underdeveloped. Most gray-zone scholarship focuses on kinetic or political dimensions, while maritime cybersecurity research has primarily examined technical vulnerabilities, risk, and operational resilience. Less attention has been given to how fragmented governance may enable gray-zone cyber activity. This study

addresses that intersection.

2.2 IT/OT Convergence and the Maritime Cyber-Threat Landscape

The convergence of IT and OT systems in the MTS has been a significant structural change in maritime operations over the past decade. IT systems handling data processing, business communications, and logistics coordination have become increasingly integrated with OT systems that directly control physical processes including engine management, ballast control, crane automation, and navigation equipment (Martin & Benson, 2023). This convergence offers operational efficiency gains but creates interconnected attack surfaces in which a digital compromise can translate into physical consequences affecting vessel movement, port operations, and safety-critical systems.

Martin and Benson (2023) observe that maritime OT environments present unique challenges relative to land-based industrial control systems. These include the difficulty of patching legacy equipment at sea, the absence of dedicated on-board cybersecurity expertise, and the physical isolation of vessels during voyages. These conditions may allow cyber compromises to persist for extended periods before detection. The same study notes that the regulatory frameworks governing maritime OT security lag significantly behind those applicable to onshore critical infrastructure sectors such as energy or water, a gap that the literature has not yet adequately addressed.

Empirical research with deck officers also shows significant differences in perceived cyber risk between vessel IT and OT systems, with cybersecurity training associated with greater OT risk awareness (Haugli-Sandvik et al., 2024).

The maritime sector has undergone rapid digital transformation, integrating electronic navigation systems, automated cargo platforms, port community systems, and satellite communications into operational workflows that were historically analog or isolated (Afenyo & Caesar, 2023). That transformation has coincided with an increase in reported cyber incidents spanning a wide range of attack types. Akpan et al. (2022) identify several recurring threat categories, including unauthorized access to navigation systems, manipulation of cargo data, ransomware targeting port terminals, and interference with automatic identification systems (AIS), while Schwarz et al. (2021) document ransomware, AIS manipulation, GPS spoofing and jamming, and supply-chain-related attacks, each of which has the potential to disrupt interconnected maritime systems in ways that extend beyond conventional IT compromise. A further complication noted by Afenyo and Caesar (2023) is that real-time threat data for the maritime sector remains sparse, partly reflecting gaps in standardized reporting. Analysis of recorded maritime cyber incidents over two decades further demonstrates dependencies among multiple cybersecurity risk factors rather than isolated technical causes (Mohsendokht et al., 2024). Without mandatory, standardized incident reporting, the full scope of maritime cyber threats is likely underestimated. Port-focused empirical research similarly indicates that cybersecurity exposure reflects interacting human, infrastructure, and procedural factors rather than technical vulnerabilities alone (Senarak, 2021).

These technical and operational risks are further complicated by governance and regulatory fragmentation.

2.3 Governance and Regulatory Fragmentation

Governance vulnerabilities arise when overlapping jurisdictions, uneven framework coverage, and inconsistent implementation leave responsibility and cybersecurity expectations unclear across maritime stakeholders.

International and national bodies have produced a range of guidance documents, standards, and regulations addressing maritime cyber risk, and Table 2 synthesizes the major frameworks according to scope, binding authority, enforcement mechanism, and identified limitations. As illustrated, no single framework provides comprehensive, enforceable coverage across the entire MTS ecosystem. Flag state discretion under IMO guidance, the exclusion of the existing fleet from IACS requirements, and the jurisdictional limits of the USCG rule collectively produce a fragmented governance landscape. A vessel may therefore meet one framework while remaining outside the scope of others, and interactions between frameworks are rarely defined. This regulatory patchwork may create conditions favorable to

gray-zone activity. Similar patterns of fragmented authority producing uneven implementation have been documented in broader cybersecurity governance research (Mirzaei, 2024; Public-Private Analytic Exchange Program, 2024).

Framework	Issuing Body	Scope	Binding?	Enforcement Mechanism	Key Gaps	Gray-Zone Relevance
MSC-FAL.1/Circ.3/Rev.3	IMO	International shipping (flag states)	Non-binding guidance	Flag state implementation	No verification mechanism; implementation varies by flag state	Variable flag-state implementation may create uneven cybersecurity baselines and enforcement gaps.
IACS UR E26 (2023)	IACS	Newbuild vessels from July 2024	Binding for member class societies	Classification survey	Applies only to newbuilds; legacy fleet excluded	Exclusion of much of the legacy fleet may leave older vessels subject to less consistent cybersecurity requirements
IACS UR E27 (2023)	IACS	Onboard systems and equipment	Binding for member class societies	Classification survey	Equipment vendors may operate outside IACS jurisdiction	Vendor and equipment coverage gaps may create inconsistent protection across interconnected onboard systems.
USCG Final Rule (2025)	U.S. Coast Guard	U.S.-flagged vessels, MTSA facilities, OCS facilities	Binding (U.S. jurisdiction)	USCG inspection	Limited to U.S.-flagged and U.S.-port-calling vessels	Jurisdictional limits may leave jurisdictional gaps across multinational vessel and port operations.
ENISA NIS2 Technical Implementation Guidance	ENISA	EU port operators and critical entities (NIS2)	Binding	NCA enforcement (NIS2)	Covers entities in scope of NIS2; broader transposition across member states has been uneven	Uneven national implementation may produce inconsistent requirements across EU maritime entities.

Table 2. Comparison of major maritime cybersecurity regulatory frameworks (Sources: IMO, MSC-FAL.1/Circ.3/Rev.3; IACS (2023a, 2023b); USCG (2025); ENISA (2025))

These differences create jurisdictional and implementation seams that may increase ambiguity over applicable requirements, enforcement responsibility, and incident coordination, thereby creating conditions favorable to gray-zone activity.

At the organizational level, case-study evidence also shows that cybersecurity implementation requires translating regulatory expectations into company procedures, audits, gap assessment, and risk-mitigation practices (Kechagias et al., 2022).

This study therefore examines governance fragmentation as a distinct cyber-risk layer that interacts with, rather than replaces, technical vulnerabilities.

3. TRM PROCESS AND THE CONCEPTUAL MODEL

In this section, authors propose a conceptual model after summarizing the TRM process. The conceptual model, The Vulnerability Cycle for Gray-Zone Activities, is built on findings of the Maritime Transportation System (MTS) Cybersecurity TRM.

All TRM process details are not shared here; instead, authors use the expert-derived findings to examine how fragmented regulation and uneven cybersecurity implementation create conditions under which gray-zone cyber operations can be conducted against vessels, ports, and maritime supply chains.

3.1 TRM Process

The roadmap was developed through a one-year effort led by the Maritime Cybersecurity Applied Research, Technology and Education Center (MCARTEC) at the University of North Carolina Wilmington (CCDE, 2025), using the NIST CSF 2.0 as an organizing framework across governance and technical dimensions of maritime cybersecurity.

Data collection proceeded through three structured workshops: a stakeholder workshop in October 2024 and two additional workshops in January and March 2025. Participants were subject matter experts from academia, government, industry, the military, and research organizations, recruited internationally by the MCARTEC team. Working groups were organized around the six NIST CSF 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover.

The engagement process summarized in Table 3 was designed to surface recurring themes in maritime cybersecurity capability across stakeholder groups and NIST CSF 2.0 functional areas. Findings were interpreted by treating governance, organizational, personnel, and technological dimensions as interacting contributors to cyber resilience.

The MCARTEC team recruited a pool of 38 MTS experts from international academic, government, military, national laboratory, maritime, and cybersecurity organizations. Workshop attendance was 19, 15, and 17 SMEs, respectively, with participants drawn repeatedly from this expert pool across the three workshops.

The workshops were conducted on October 3, 2024; January 28, 30, and 31, 2025; and March 18–20, 2025, with participating organizations representing the United States and several European countries.

Participants worked in groups aligned with paired NIST CSF 2.0 functions and generated inputs through brainstorming, structured discussions, index cards, and collaborative whiteboards. The TRM analysis proceeded from Drivers → Capability Gaps → Technology Characteristics → R&D Programs: drivers were identified first, their strategic needs defined capability gaps, and technology characteristics were developed to address those gaps through structured R&D programs.

Component	Description
Total experts recruited	38 worldwide SMEs
Stakeholder workshop participants	19 SMEs
Workshop 1 participants	15 SMEs
Workshop 2 participants	17 SMEs
Organizational representation	Academia, industry, government agencies, national laboratories, military organizations, maritime operational organizations
Workshop period	October 2024 – March 2025
Framework guiding analysis	NIST CSF 2.0 (Govern, Identify, Protect, Detect, Respond, Recover)
Group organization	Participants assigned to paired NIST CSF functions
Data collection mechanisms	Brainstorming sessions, structured discussions, index cards, collaborative whiteboard activities
Prioritization approach	Voting and iterative expert review
Analytical process	Drivers → Capability Gaps → Technology Characteristics → R&D Programs
Validation approach	Multiple workshop iterations and cross-sector expert triangulation
Roadmapping output	44 R&D program areas, 153 key research questions
Supporting evidence generated	122 drivers, 97 capability gaps, 69 technology characteristics

Table 1. Subject matter expert engagement and TRM process summary

3.2 Identification of the TRM Themes Specific to Gray-Zone Activities

The current study conducted a secondary qualitative analysis of findings reported in the MTS Cybersecurity TRM rather than a reanalysis of individual workshop transcripts or participant-level responses.

The roadmap identifies 44 R&D program areas representing areas requiring further research and development. To develop the conceptual model, the authors selected TRM findings relevant to the research questions and gray-zone literature, yielding nine themes: fragmented cyber authority, weak enforcement, inter-agency coordination, workforce readiness, IT/OT asset visibility, centralized monitoring, incident response, recovery, and governance.

Using qualitative content analysis, the authors compared selected TRM findings with the research questions and gray-zone literature and grouped conceptually similar findings into four problem areas: fragmented governance, personnel and organizational readiness, technical visibility and monitoring, and response and recovery. This secondary analysis did not use SME-level frequency coding; therefore, the categories represent analytical groupings rather than prevalence estimates. This mapping allows systematic comparison of capability maturity across NIST CSF 2.0 functions. Table 4 also shows the coverage of topics for each category as identified by the TRM process.

Problem Areas	Coverage	Relevant NIST CSF 2.0 Function
Fragmented governance	Unclear authority, inconsistent standards, weak enforcement, certification gaps, poor industry-government alignment	Govern
Limitations in personnel and organizational readiness	Leadership awareness, role-specific training, cyber-literate workforce capacity	Govern, Protect
Technical visibility and monitoring gaps	Monitoring capabilities, IT/OT asset management, cyber-physical mapping, intrusion detection, forensic data collection	Detect, Identify
Response and recovery weaknesses	Incident-response coordination, recovery design	Respond, Recover

Table 4. TRM findings related to gray-zone cybersecurity

From a maritime cybersecurity perspective, these areas span governance, human, technical, and operational dimensions, reflecting the interdependence of vessels, ports, shore systems, and cross-jurisdictional response.

These themes span multiple NIST CSF 2.0 functional areas, suggesting that the identified vulnerabilities extend beyond a single technical or organizational domain.

One of the major findings is that maritime cybersecurity governance remains fragmented across agencies, standards bodies, and operational stakeholders. The roadmap identified poor industry-government alignment as a consistent barrier to cybersecurity information sharing, effective regulation, and technology adoption. A related governance gap concerns certification and accreditation: the roadmap notes a lack of established programs for validating technologies deployed into the MTS, suggesting that regulatory fragmentation affects not only policy but also technology procurement, system validation, and trust in maritime IT/OT equipment.

Another major finding is that workforce and leadership limitations weaken maritime cyber resilience. The roadmap identifies a shortage of cyber-literate personnel across both technical and operational roles; a gap that is particularly significant in maritime environments where a cyber compromise may manifest through physical systems including navigation, cargo movement, and communications. The roadmap also points to insufficient role-specific cybersecurity training, poor cybersecurity awareness among ship crews and office staff, and unclear cybersecurity ownership aboard vessels, exacerbated by high crew turnover.

Many maritime organizations lack the technical visibility needed to identify and respond to cyber threats in a timely manner. The TRM identifies gaps in vulnerability scanning, IT/OT asset management, centralized monitoring, and incomplete asset records across maritime environments (CCDE, 2025).

The TRM identifies gaps in response authority, coordinated incident procedures, forensic visibility, and recovery planning (CCDE, 2025). The roadmap highlights needs for clearer response roles, improved ship-to-shore communication during incident response, and stronger forensic data collection. These gaps reflect the realities of operating at sea, where communication may be limited and cyber incidents can affect both digital and physical systems, meaning that maritime cyber recovery is not simply a technical process of restoring systems but also involves maintaining operations, protecting critical data, and ensuring safe resumption of activity.

Rather than causing obvious physical destruction, a gray-zone adversary may disrupt cargo systems, delay port operations, interfere with communications, manipulate data, or degrade confidence in maritime services. Such activity may appear at first to be a technical malfunction, a software failure, or a routine operational delay. When reporting channels and response authorities are unclear, valuable time may be lost before the incident is identified as malicious.

Governance ambiguity may create favorable conditions for gray-zone activity because adversaries

ISSN: 2473-4901
v12 n6744

frequently rely on uncertainty, delayed attribution, and unclear response responsibilities. A cyber incident affecting a vessel, port subsystem, or logistics platform may remain unresolved while stakeholders determine who has investigative authority, who is responsible for reporting, and who owns the operational response. Real-world maritime cyber incidents further illustrate how cyber disruptions can generate operational and strategic consequences beyond isolated technical failures. The 2017 NotPetya attack, which affected Maersk's booking and logistics systems and contributed to operational impacts across port and shipping activities, demonstrated how a cyber incident affecting a single organization can propagate through interconnected maritime networks (Abbatemarco et al., 2024; Schwarz et al., 2021). Research examining maritime cyber incidents has similarly documented GPS interference, AIS spoofing events, and navigation-system manipulation cases as examples of the susceptibility of maritime cyber-physical systems to disruptions beyond traditional IT compromise (Schwarz et al., 2021). These incidents collectively suggest that maritime cyber risks increasingly involve operational disruption, cascading consequences, and uncertainty rather than only direct system damage.

Recovery can also be understood as a strategic security function, not only an operational or technical process. In a gray-zone context, an adversary's objective may be to prolong disruption rather than cause permanent damage. A temporary interruption in port operations, cargo processing, or vessel communications can still produce wider economic and security effects if recovery is slow. The roadmap's focus on recovery procedures, business continuity, disaster recovery, restoration of critical data, and design for recovery reflects the need to treat recovery planning as a core component of maritime cybersecurity resilience.

3.3 Conceptual Model Based on the TRM Findings

Building on the four problem areas identified in Section 3.2, the authors translated their relationships into the Vulnerability Cycle for Gray-Zone Activities shown in Figure 1. The model links governance fragmentation to uneven security baselines, detection blind spots, extended detection windows, and delayed response.

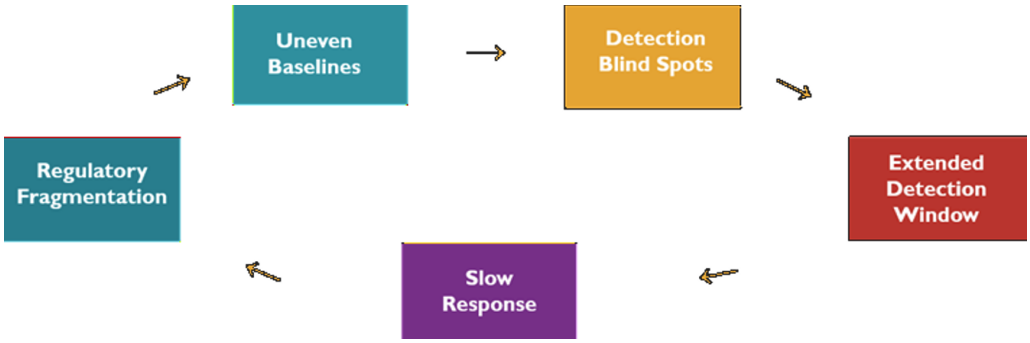

Figure 1. The Vulnerability Cycle for Gray-Zone Activities

Slow or fragmented response may limit shared incident documentation, lessons learned, and evidence available for regulatory adaptation. This relationship is therefore treated as a reinforcing mechanism rather than a direct causal claim; broader institutional, political, and governance factors may also sustain regulatory fragmentation.

From a maritime cybersecurity perspective, the cycle illustrates how fragmented authority and uneven cybersecurity practices across interconnected vessels, ports, and shore systems may allow localized weaknesses to delay collective detection and coordinated response.

The five constructs operationalize relationships among the four problem areas identified in Section 3.2. These five main constructs create five relationships between them and eventually create a cycle. The cycle works as follows:

For the flow from the Regulatory Fragmentation to Uneven Baselines: Because no single enforceable framework covers all MTS stakeholders, different organizations implement cybersecurity to different

standards. A vessel operator, a port authority, and a terminal operator serving the same supply chain may each have entirely different security postures.

For the flow from Uneven Baselines to Detection Blind Spots: When security baselines are uneven, the weakest-postured organizations create gaps in collective visibility. An incident that begins in an unmonitored or under-monitored subsystem, such as a vendor-managed system, a legacy OT environment, a small port operator, goes undetected not because detection is technically impossible but because no one with detection capability is watching that specific system.

For the flow from Detection Blind Spots to the Extended Detection Window: Extended monitoring gaps may allow an adversary to maintain access or cause disruption for longer before detection. In a fragmented environment with blind spots, an anomaly may persist for days or weeks before it surfaces, if it surfaces at all.

For the flow from the Extended Detection Window to the Slow Response: Delayed detection can constrain the timeliness of incident response. But the problem compounds: by the time the incident is identified, the responsible parties still have to determine who has authority to respond, who coordinates with whom, and what the response protocol is.

For the flow from Slow Response back to Regulatory Fragmentation: Slow or fragmented response may limit shared incident documentation, lessons learned, and evidence supporting regulatory adaptation. This feedback may reinforce existing fragmentation, although broader institutional, political, and governance factors also influence regulatory change.

4. DISCUSSIONS AND RECOMMENDATIONS

The recommendations below are derived from the four problem areas identified through the TRM analysis in Section 3.2 and are supported, where applicable, by regulatory and scholarly literature. Recommendations extending beyond these sources are presented as author-proposed implications.

4.1 Regulatory Harmonization

Consistent with the fragmented-governance findings, the first priority is to reduce fragmentation across existing maritime cybersecurity frameworks. The varying scope, enforcement authority, jurisdiction, and applicability of frameworks create uneven cybersecurity expectations across flag states, port states, vessel operators, and technology vendors.

Based on these findings, we propose that the international community work toward translating IMO cyber guidance into binding instruments through flag state implementation (IMO, 2024). Minimum expectations for asset inventory, cyber risk assessment, incident reporting, access control, vulnerability management, backup procedures, and recovery planning should be incorporated into flag state regulatory frameworks rather than left to voluntary adoption.

Coordination among maritime authorities across flag and port states should be strengthened to reflect the international nature of maritime supply chains. National cybersecurity rules alone may not close systemic gaps when vessels move through multiple jurisdictions with inconsistent regulatory requirements. Greater alignment among maritime authorities through bilateral and multilateral agreements, mutual recognition of cybersecurity standards, and coordinated port-state control inspection criteria would reduce jurisdictional seams.

The legacy fleet represents a significant governance gap. IACS Unified Requirements E26 and E27 apply to vessels contracted for construction from July 2024 onward (IACS, 2023a, 2023b). This leaves in-service vessels subject to the inconsistently enforced requirements of IMO guidance and domestic regulations. Recognizing that many of those vessels will remain in service for a decade or more, flag states and port state control authorities should work toward extending equivalent cybersecurity expectations to existing vessels through a realistic phase-in timeline.

Finally, maritime cybersecurity regulation can draw lessons from models such as NERC CIP in the North American energy sector and the EU's NIS2 framework. Both models illustrate approaches based on

mandatory cybersecurity requirements and defined accountability mechanisms (Mirzaei, 2024). While the maritime sector does not need to replicate these models exactly, the underlying principle is applicable. Enforceable minimum standards, paired with independent verification and standardized reporting, may reduce stakeholder variance and strengthen accountability.

4.2 Governance and Enforcement

The TRM findings on unclear authority and weak industry-government alignment support strengthening governance and enforcement mechanisms. The findings show that unclear authority, inconsistent enforcement, and weak industry-government alignment can delay incident detection and response. In a gray-zone context such delays are strategically significant because adversaries may seek to create disruption without immediately revealing malicious intent.

Based on these findings, we propose clearer lines of cyber authority across maritime agencies. Such an initiative would clarify responsibility for investigation, reporting, operational coordination, public communication, and recovery support during a maritime cyber incident. This would be particularly useful when incidents affect both vessel systems and port operations or when disruptions cross national boundaries.

The identified reporting and coordination gaps also support more standardized incident reporting mechanisms across flag and port states, since inconsistent reporting makes it difficult to identify patterns of malicious activity, assess sector-wide risk, or detect coordinated gray-zone campaigns. Reporting requirements should define what must be reported, when it must be reported, who receives the report, and how sensitive information will be protected, providing the specificity that current guidance lacks and improving shared situational awareness across the sector.

Based on the identified cross-jurisdictional coordination gaps, we propose exploring an international maritime ISAC, a sector-specific, cross-border information sharing and analysis structure that could aggregate threat intelligence, coordinate incident response across jurisdictions, and provide the sector-level pattern recognition that no single national body can achieve alone. While national-level bodies such as the MTS-ISAC provide a foundation, the inherently international character of maritime operations requires a cross-border structure capable of detecting coordinated gray-zone campaigns deliberately designed to remain below the visibility threshold of any individual organization or national authority. Critical infrastructure research similarly emphasizes that public-private coordination is essential to strengthening cybersecurity in sectors characterized by fragmented responsibilities (Carr, 2016).

4.3 Workforce Readiness

The identified personnel and organizational readiness gaps support improving maritime cybersecurity workforce readiness. When personnel across vessels, ports, and shore-based organizations lack role-specific cyber knowledge, incidents may be misread as routine technical failures — compounding the detection delays that gray-zone adversaries rely on.

One potential response is the development of maritime-specific cybersecurity certification programs to address the unique characteristics of maritime environments, including IT/OT convergence, vessel operations, port systems, navigation technologies, cargo platforms, and cyber-physical risk. This would provide a common knowledge baseline for cybersecurity professionals working in maritime settings that general-purpose credentials do not supply.

The identified readiness gaps also support role-specific training for crews and leadership: crew members need practical training on cyber hygiene, anomaly recognition, reporting procedures, and operating under degraded conditions. Port and terminal personnel need training on IT/OT dependencies, incident escalation, and coordination with outside partners. Senior leaders need training on governance, investment decisions, regulatory obligations, business continuity, and strategic cyber risk.

We further propose integrating cyber awareness into maritime licensing curricula. This would ensure that cybersecurity becomes part of professional maritime education, and that as vessels and ports become increasingly digitized, cyber awareness is treated as a core safety and security competency.

4.4 Technical Capability

The identified visibility and monitoring gaps support improving technical capability across vessels, ports, and maritime support systems. The TRM identifies gaps in IT/OT visibility and asset management across maritime environments. Without accurate asset inventories, operators may not know which systems are exposed, which are critical, or how a cyber incident could affect physical operations. Deployment of automated IT/OT asset management across vessels and ports would help organizations identify connected systems, monitor configuration changes, detect unauthorized devices, and prioritize protection for mission-critical assets. This capability is especially important for legacy systems and vendor-managed technologies that may not be fully documented.

The TRM findings also support development of centralized maritime cyber-state monitoring capabilities. Such an initiative could provide a clearer picture of cyber conditions across ports, vessels, logistics systems, and supporting organizations. This type of infrastructure would not require every organization to expose sensitive internal data but would require mechanisms for sharing relevant indicators, alerts, operational impacts, and recovery status. Improved monitoring could help distinguish isolated technical failures from coordinated gray-zone activity.

Finally, the identified response, recovery, and training gaps support further investment in maritime-specific recovery tools and cyber ranges. Recovery capabilities should include restoration procedures for critical ship and port systems, backup validation, forensic data preservation, manual fallback procedures, and decision-support tools for operating during cyber disruption. Cyber ranges would allow maritime organizations to test response plans, train personnel, and simulate gray-zone scenarios in a controlled environment.

5. CONCLUSIONS

This paper argued that regulatory fragmentation increases the MTS's vulnerability to gray-zone cyber threats. Findings from the MTS TRM show that unclear authority, inconsistent enforcement, limited cyber-literate personnel, weak IT/OT asset visibility, and immature response and recovery processes create exploitable gaps across vessels, ports, and supply chains. These weaknesses are especially serious in gray-zone contexts, where adversaries can use ambiguity, delayed attribution, and uneven coordination to cause disruption without clearly crossing into conventional conflict.

The central conceptual contribution of this study is the argument that governance gaps should be understood as cybersecurity attack surfaces. Regulatory fragmentation is not merely an administrative deficiency; it is a strategic vulnerability that gray-zone actors can exploit to create disruption while remaining below the threshold of conventional military response. In this environment, cyber incidents may not immediately appear to be hostile acts, as they may look like technical failures, operational delays, communications outages, cargo-processing problems, or system malfunctions. This ambiguity can delay detection, reporting, attribution, and coordinated response.

5.1 Implications and Future Work

These governance imperatives are not unique to maritime cybersecurity. Frameworks such as NERC CIP in the North American energy sector and NIS2 in the European Union demonstrate how enforceable cybersecurity baselines can reduce stakeholder variance and improve accountability, and the maritime sector, which carries more than 80% of the volume of international trade, lacks an equivalent comprehensive baseline. Developing a more consistent maritime cybersecurity governance model should therefore be a priority for policymakers, regulators, and industry partners.

Future research should build on these findings by developing maritime cybersecurity maturity models, conducting quantitative analysis of the relationship between compliance and incident outcomes, comparing flag-state cyber governance approaches, and designing maritime-specific recovery tools. Such work would strengthen the ability of the MTS to detect, respond to, and recover from gray-zone cyber threats before localized disruptions cascade into broader economic and national security consequences. The governance structure, legal framework, funding model, and operational design of an international maritime ISAC also warrant dedicated research. This is especially important because there is no cross-border, sector-specific way to share information today, and national bodies on their own

cannot solve the coordination challenges that span multiple countries.

There are a few limitations of this study. First, the roadmap findings originate from a single research initiative, and while expert triangulation across workshops reduces individual bias, the findings reflect only the opinions of the participating subject matter experts and may not represent all regions of the global MTS. Second, qualitative synthesis does not allow statistical generalization, and the findings reflect the perspectives of a specific expert community rather than prevalence across the broader MTS.

6. ACKNOWLEDGEMENTS

This work was supported by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST) under Financial Assistance Award No. 60NANB24D144. Additional support was provided by the UNCW Office of Research and Innovation through the Research Hub Award for MCARTEC (2024–2026) and the Carolina Cyber Network Sector Leadership grants.

7. AI DISCLOSURE STATEMENT

The authors used Claude Sonnet (Anthropic) during the preparation of this manuscript solely for language refinement, specifically to improve grammatical accuracy and sentence fluency. No content was generated by AI; all ideas, arguments, and conclusions are the authors' own. All AI suggestions were reviewed and verified by the authors, who take full responsibility for the accuracy and integrity of this work.

8. REFERENCES

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

Abbatemarco, N., Salviotti, G., D'Ignazio, C., & De Rossi, L. M. (2024). Understanding leadership competencies in cyber crisis management: Insights from the maersk global supply chain meltdown. https://doi.org/10.24251/HICSS.2024.508

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.

Carr, M. (2016). *Public–private partnerships in national cyber-security strategies*, International Affairs, Volume 92, Issue 1, Pages 43–62, https://doi.org/10.1111/1468-2346.12504.

Center for Cyber Defense Education (CCDE). (2025). *Maritime Transportation System (MTS) cybersecurity technology roadmap (Version 1)*. University of North Carolina Wilmington. https://hdl.handle.net/20.500.14481/1433

European Union Agency for Cybersecurity (ENISA). (2025). *Technical implementation guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures* (Version 1.0). Publications Office of the European Union. https://doi.org/10.2824/2702548.

Ferazza, F., & Mersinas, K. (2025). Non-kinetic naval strategy: the role of cyber operations in modern maritime conflict. Journal of Cybersecurity, 11(1), tyaf031. https://doi.org/10.1093/cybsec/tyaf031

Haugli-Sandvik, M., Lund, M. S., & Bjørneseth, F. B. (2024). Maritime decision-makers and cyber security: Deck officers' perception of cyber risks towards IT and OT systems. *International Journal of Information Security, 23*, 1721–1739. https://doi.org/10.1007/s10207-023-00810-y

International Association of Classification Societies. (2023a). *Unified Requirement E26: Cyber resilience of ships (Rev. 1).* IACS.

International Association of Classification Societies. (2023b). *Unified Requirement E27: Cyber resilience of on-board systems and equipment (Rev. 1).* IACS.

International Maritime Organization. (2024). *Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.3).* International Maritime Organization.

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

Letts, D. (2024). The maritime domain. In M. Regan & A. Sari (Eds.), Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies (pp. 251–270). Oxford University Press.

Martin, L., & Benson, B. (2023). *ICS/OT cybersecurity considerations for maritime transportation: Threats, challenges, and the need for a standardized approach* [White paper]. Dragos, Inc. and ABS Group.

Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict.* United States Army War College Press.

Mirzaei, P. (2024). The new F-word: The case of fragmentation in Dutch cybersecurity governance. Computer Law & Security Review, 55.

Mohsendokht, M., Li, H., Kontovas, C., Chang, C.-H., Qu, Z., & Yang, Z. (2024). Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades. *Ocean Engineering, 312*, 119078. https://doi.org/10.1016/j.oceaneng.2024.119078

Public-Private Analytic Exchange Program. (2024). *U.S. maritime trade and port cybersecurity: Shoring up maritime cybersecurity – Enhancing cybersecurity and resilience.* U.S. Department of Homeland Security.

Schwarz, M., Marx, M., & Federrath, H. (2021). A structured analysis of information security incidents in the maritime sector. arXiv preprint. https://doi.org/10.48550/arXiv.2112.06545

Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. *The Asian Journal of Shipping and Logistics, 37*(1), 20–36. https://doi.org/10.1016/j.ajsl.2020.05.001

United States Coast Guard. (2025). *Cybersecurity in the Marine Transportation System: Final rule, 90 FR 6298. Federal Register*.

United Nations Trade and Development. (2024). *Review of maritime transport 2024*. United Nations Trade and Development